第41卷第7期 中国科学技术大学学报 Vol. 41, No. 7
2011年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2011

文章编号:0253-2778(2011)07-0615-04

抗合谋攻击的多变量群签名方案

陶 羽[1,2],杨亚涛[2],李子臣[2],郑 昕[1,2]

(1.西安电子科技大学通信工程学院,陕西西安 710071;2.北京电子科技学院,北京 100070)

摘要:多变量公钥密码体制能抵御量子计算机的攻击,被认为是后量子时代的一种安全的密码体制备选方案.提出了一种基于多变量公钥密码体制的群签名设计模型,同时在分析该方案时,提出了一种合谋攻击方案,可以有若干合谋攻击者对群签名体制进行伪造签名攻击.随后,给出了一种新的矩阵乘法定义,以及素矩阵等概念,并提出了一种可以抵抗合谋攻击的基于多变量公钥密码体制的群签名设计模型.分析结果表明:该方案不仅能够从根本上抵抗合谋攻击和伪造签名攻击,而且在保证匿名性的前提下,能够真正实现签名成员身份的可追查性,同时通过构造安全的密钥生成协议保证群签名私钥的不可知性,因此具有更高的安全性.

关键词:多变量;群签名;合谋攻击;伪造签名攻击

中图分类号:TP393.08 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.07.008

Multivariate group signature scheme withstanding conspiracy attacks

TAO Yu[1,2], YANG Yatao[2], LI Zichen[2], ZHENG Xin[1,2]

(1. *Communication Engineering Institute, Xidian University, Xi'an* 710071, *China*;
2. *Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*)

Abstract: Multivariate public key encryption scheme which can resist attacks by quantum computer is believed to be an alternative security cryptography scheme in the post-quantum age. A multivariate group signature scheme was proposed. After an analysis of the scheme, a conspiracy attack scheme which could offer forgery attacks to the signature system was proposed. Then, a new matrix multiplication definition and prime matrix concept were given, and a conspiracy attack immune group signature scheme was proposed. Analysis shows that the scheme can not only fundamentally withstand conspiracy and forgery attacks, but trace the identity of signature members anonymously. Meanwhile, it can realize the unknown ability of group signature secret keys by constructing a secure distributed key generation protocol, thus greatly enhancing group signature security.

Key words: multivariate; group signature; conspiracy attack; forgery attack

0 引言

群签名,即群数字签名,最先由 Chaum 等[1]于1991年提出.在群签名方案中,一个群体中的成员可代表整个群体签名,群签名是可以公开验证的,每个成员的群签名均可用统一的群公钥来验证,而且

收稿日期:2011-05-04;**修回日期**:2011-06-21

基金项目:国家自然科学基金(61070219),北京电子科技学院信息安全重点实验室项目资助.

作者简介:陶羽,男,1987年生,硕士生. 研究方向:后量子签名体制. E-mail: Taoyu1987@sohu.com

通讯作者:杨亚涛,博士. E-mail:yyt2011@gmail.com

对于给定的信息和签名，只有群体管理员才能确定签名者的身份. 合谋攻击是指，当群中 t 个或更多的恶意成员合谋时，就可以恢复群秘密多项式，从而获得群密钥和其他成员的私钥，因此群内的一组成员可以假冒另一组成员进行签名. 许多学者对如何抵抗合谋攻击做了大量研究，但合谋攻击一直是群签名体制中难以解决的问题.

多变量公钥密码体制能抵御量子计算机的攻击，被认为是后量子时代的一种安全的密码体制备选方案. 其在管理、军事、政治及经济等许多方面有着广泛的应用前景，因此基于多变量的群签名方案极具潜力，具有重要的研究意义.

1 多变量群签名设计

1.1 多变量群签名模型

（Ⅰ）签名模型结构图

$$\text{签名值 } s=(s_1,s_2,\cdots,s_n)\underset{U^{-1}}{\overset{U}{\rightleftharpoons}}x\underset{Q^{-1}}{\overset{Q}{\rightleftharpoons}}$$

$$z_1\underset{T_1^{-1}}{\overset{T_1}{\rightleftharpoons}}z_2\underset{T_2^{-1}}{\overset{T_2}{\rightleftharpoons}}z_3\cdots z_n\underset{T_n^{-1}}{\overset{T_n}{\rightleftharpoons}}y\underset{N^{-1}}{\overset{N}{\rightleftharpoons}}$$

$$m=(m_1,m_2,\cdots,m_m)\text{ 消息值}$$

其中公钥为 $P=U\circ Q\circ T_1\circ T_2\circ\cdots\circ T_n\circ N$；私钥为 U，Q，T_i，N.

（Ⅱ）签名生成过程

计算签名需利用陷门信息(U,Q,N)的逆映射(U^{-1},Q^{-1},N^{-1}). 由于 U,N 为仿射变换，因此

$$N^{-1}(x)=M_N^{-1}(x-c_N),$$

$$U^{-1}(x)=M_U^{-1}(x-c_U).$$

Q^{-1}的计算则需根据 Q 的具体结构来确定. $T_1,T_2,\cdots,T_n$ 为群管理员设计出的 n 个可逆仿射变换，并将其分别分发给群签名成员 $A_1,A_2,\cdots,A_n$，群管理员记录私钥与成员的对应关系. 设 m 是消息 M 的消息值，则

①计算全体群签名成员签名私钥的合成映射 $T=T_1\cdot T_2\cdot\cdots\cdot T_n$；

②计算出映射 T 的逆变换 T^{-1}；

③根据私钥$(U^{-1},Q^{-1},N^{-1},T^{-1})$依次计算 $y=N^{-1}(m)$，$z_1=T^{-1}(y)$，$x=Q^{-1}(z_1)$和 $s=U^{-1}(x)$；

④最终得到 $s=(s_1,s_2,\cdots,s_n)$即为签名值.

（Ⅲ）验证签名过程

$s=(s_1,s_2,\cdots,s_n)$为签名者发送来的签名值，验证者计算公钥方程 $P=U\circ Q\circ T\circ N$ 的函数值 $(p_1(s_1,\cdots,s_n),\cdots,p_m(s_1,\cdots,s_n))$，判断是否与原消息值 $m=(m_1,m_2,\cdots,m_m)$一致，相同即为合法，否则视为无效签名.

1.2 合谋攻击

经分析，前面提出的多变量群签名模型存在安全隐患，可以被合谋攻击.

设群签名中有 $2n$ 名群成员，分别为 $A_1,A_2,\cdots,A_n,B_1,B_2,\cdots,B_n$，其签名私钥分别为 $T_{A_1},T_{A_2},\cdots,T_{A_n},T_{B_1},T_{B_2},\cdots,T_{B_n}$. 假设群签名成员中 $A_1,A_2,\cdots,A_n$ 为合谋攻击者，他们可以找到仿射变换 $H_{A_1},H_{A_2},\cdots,H_{A_n}$，使得 $H_{A_1}\cdot H_{A_2}\cdot\cdots\cdot H_{A_n}=T_{A_1}\cdot T_{A_2}\cdot\cdots\cdot T_{A_n}$. 当发动合谋攻击时，合谋者 $A_1,A_2,\cdots,A_n$ 将 $H_{A_1},H_{A_2},\cdots,H_{A_n}$作为他们的私钥进行签名，则验证者验证此签名依旧有效. 但追查签名时，查得该签名的签名私钥分别为 $H_{A_1},H_{A_2},\cdots,H_{A_n},T_{B_1},T_{B_2},\cdots,T_{B_n}$，其中追踪到 $T_{B_1},T_{B_2},\cdots,T_{B_n}$分别是群签名成员 $B_1,B_2,\cdots,B_n$ 的签名私钥，而却追踪不到 $H_{A_1},H_{A_2},\cdots,H_{A_n}$的签名人. 因此签名者 $A_1,A_2,\cdots,A_n$ 签名有效却逃脱了责任，完成了合谋攻击.

此外，群签名管理者在计算私钥的合成 $T=T_1\cdot T_2\cdot\cdots\cdot T_n$ 时，因掌握所有群成员私钥的对应关系，而可能造成伪造群成员签名且无法从签名中追诉身份. 例如个别群成员没有进行签名，但群签名管理者可以利用其掌握的私钥进行伪造群成员签名，进而签名成功却无法从签名中追诉身份.

有了合谋攻击方法，前面的群签名就是不安全的. 下面介绍改进的多变量群签名方案.

2 抗合谋攻击的多变量群签名方案

本节提出一种基于多变量公钥密码体制的群签名方案，可以抵抗合谋攻击.

2.1 预备知识

首先介绍几个定义和定理.

定义 2.1（矩阵点乘法） 定义如下矩阵点乘法规则：

$$\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\&\cdots\cdots\cdots&&\\a_{n1}&a_{2n}&\cdots&a_{mn}\end{pmatrix}\cdot\begin{pmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\&\cdots\cdots\cdots&&\\b_{n1}&b_{2n}&\cdots&b_{mn}\end{pmatrix}=$$

$$\begin{pmatrix}a_{11}b_{11}&a_{12}b_{12}&\cdots&a_{1n}b_{1n}\\a_{21}b_{21}&a_{22}b_{22}&\cdots&a_{2n}b_{2n}\\&\cdots\cdots\cdots&&\\a_{n1}b_{n1}&a_{2n}b_{2n}&\cdots&a_{mn}b_{mn}\end{pmatrix}$$

即矩阵点乘时，对应位置的元素进行乘法运算后，保存在相应位置上. 记为 $\mathbf{A}\cdot\mathbf{B}=\mathbf{C}$，其中

$\mathbf{A}=(a_{ij})_{n\times n}$，$\mathbf{B}=(b_{ij})_{n\times n}$，$\mathbf{C}=(a_{ij}b_{ij})_{n\times n}$.

定义 2.2（素矩阵）　形如如下的矩阵

$$\mathbf{A}=(a_{ij})_{n\times n}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots\cdots\cdots & & \\ a_{n1} & a_{2n} & \cdots & a_{mn} \end{pmatrix},$$

其中每个元素 a_{ij} 都为素数，这样组成的矩阵称为素矩阵.

定义 2.3（因子矩阵）　如果矩阵 $\mathbf{C}=\mathbf{A}\cdot\mathbf{B}$，其中

$\mathbf{A}=(a_{ij})_{n\times n}$，$\mathbf{B}=(b_{ij})_{n\times n}$，$\mathbf{C}=(a_{ij}b_{ij})_{n\times n}$，

那么矩阵 $\mathbf{A},\mathbf{B}$ 称为矩阵 $\mathbf{C}$ 的因子矩阵.

定理 2.1　如果矩阵 $\mathbf{C}=\mathbf{A}\cdot\mathbf{B}$，其中矩阵 $\mathbf{A}=(a_{ij})_{n\times n}$，$\mathbf{B}=(b_{ij})_{n\times n}$ 均为素矩阵，且从矩阵 $\mathbf{A}$ 到 $\mathbf{B}$ 相应位置上的素数依次增大，那么矩阵 $\mathbf{C}=(c_{ij})_{n\times n}$ 分解出的因子矩阵是唯一的，且必为矩阵 $\mathbf{A}$ 和 $\mathbf{B}$.

证明　因为 $\mathbf{C}=\mathbf{A}\cdot\mathbf{B}$，其中矩阵 $\mathbf{A},\mathbf{B}$ 的元素 a_{ij}，b_{ij} 都是大素数，由唯一因数分解定理：每一个整数 $n>1$ 都可以用唯一的方法表示为素因数之积，不同之处至多只能是因数的次序，因此矩阵 $\mathbf{C}$ 的每个元素 $a_{ij}b_{ij}$ 分解出的素数是唯一的，并且只能是 a_{ij}，b_{ij}. 当相同位置上的素数 a_{ij}，b_{ij} 都按从小到大排序，那么矩阵 $\mathbf{C}=(c_{ij})_{n\times n}$ 分解出的因子矩阵是唯一的，且必为矩阵 $\mathbf{A}$ 和 $\mathbf{B}$.

推论 2.1　如果矩阵 $\mathbf{C}=\mathbf{A}_1\cdot\mathbf{A}_2\cdot\cdots\cdot\mathbf{A}_n$，其中矩阵 $\mathbf{A}_1=(a_{1_{ij}})_{n\times n}$，$\mathbf{A}_2=(a_{2_{ij}})_{n\times n}$，…，$\mathbf{A}_n=(a_{n_{ij}})_{n\times n}$ 均为素矩阵，且从矩阵 $\mathbf{A}_1,\mathbf{A}_2$ 到 $\mathbf{A}_n$ 相应位置上的素数依次增大，那么矩阵 $\mathbf{C}=(c_{ij})_{n\times n}$ 分解出的因子矩阵是唯一的，且必为矩阵 $\mathbf{A}_1=(a_{1_{ij}})_{n\times n}$，$\mathbf{A}_2=(a_{2_{ij}})_{n\times n}$，…，$\mathbf{A}_n=(a_{n_{ij}})_{n\times n}$.

定理 2.2　如果矩阵 $\mathbf{C}=\mathbf{A}\cdot\mathbf{B}$，其中矩阵 $\mathbf{A}=(a_{ij})_{n\times n}$，$\mathbf{B}=(b_{ij})_{n\times n}$ 均为素矩阵，且选取的每个素数足够大，则矩阵 $\mathbf{C}=(c_{ij})_{n\times n}$ 分解出因子矩阵是困难的.

证明　因为 $\mathbf{C}=\mathbf{A}\cdot\mathbf{B}$，其中矩阵 $\mathbf{A},\mathbf{B}$ 的元素 a_{ij}，b_{ij} 都是大素数，由大素数分解的困难性可知，矩阵 $\mathbf{C}$ 的每个元素 $a_{ij}b_{ij}$ 分解出 a_{ij} 和 b_{ij} 是困难的，而矩阵 $\mathbf{C}=(c_{ij})_{n\times n}$ 中有 n^2 个元素. 因此矩阵 $\mathbf{C}=(c_{ij})_{n\times n}$ 分解出因子矩阵 $\mathbf{A}=(a_{ij})_{n\times n}$，$\mathbf{B}=(b_{ij})_{n\times n}$ 是困难的.

2.2　抗合谋攻击的多变量群签名方案

设 $m=(m_1,m_2,\cdots,m_m)$ 为消息值，$s=(s_1,s_2,\cdots,s_n)$ 为签名值，公钥为 $P=\mathrm{U}\circ\mathrm{Q}\circ\mathrm{T}_1\circ\mathrm{T}_2\circ\cdots\circ\mathrm{T}_n\circ\mathrm{N}$，私钥为 $(\mathrm{U},\mathrm{Q},\mathrm{T}_i,\mathrm{N})$. 设 $\mathrm{A}_1,\mathrm{A}_2,\cdots,\mathrm{A}_n$ 为 n 名群签名成员，其签名私钥分别为 $\mathrm{T}_1,\mathrm{T}_2,\cdots,\mathrm{T}_n$，且是由素矩阵 $\mathbf{M}_1,\mathbf{M}_2,\cdots,\mathbf{M}_n$ 组成的可逆仿射变换.

（Ⅰ）签名生成过程

计算签名需利用陷门信息 $(\mathrm{U},\mathrm{Q},\mathrm{N})$ 的逆映射 $(\mathrm{U}^{-1},\mathrm{Q}^{-1},\mathrm{N}^{-1})$. 由于 U，N 为可逆仿射变换，因此

$$\mathrm{N}^{-1}(x)=\mathrm{M}_{\mathrm{N}}^{-1}(x-c_{\mathrm{N}}),$$

$$\mathrm{U}^{-1}(x)=\mathrm{M}_{\mathrm{U}}^{-1}(x-c_{\mathrm{U}}).$$

Q^{-1} 的计算则需根据 Q 的具体结构来确定. 设 m 是消息 M 的消息值，则

①接收到消息值 M 后，计算 $y=\mathrm{N}^{-1}(m)$，并发送给群签名成员；

②群签名成员接收到 y 后，分别用自己的私钥进行签名，即进行运算 $z_n=\mathrm{T}_n^{-1}(y)$，$z_{n-1}=\mathrm{T}_{n-1}^{-1}(z_n),\cdots,z_1=\mathrm{T}_1^{-1}(z_2)$，该过程可由群签名管理员设计程序分别进行计算；

③根据私钥 $(\mathrm{U}^{-1},\mathrm{Q}^{-1},\mathrm{N}^{-1})$ 计算，$x=\mathrm{Q}^{-1}(z_1)$ 和 $s=\mathrm{U}^{-1}(x)$；

④最终得到 $s=(s_1,s_2,\cdots,s_n)$ 即为签名值.

（Ⅱ）验证签名过程

$s=(s_1,s_2,\cdots,s_n)$ 为签名者发送来的签名值，验证者计算公钥方程 $P=\mathrm{U}\circ\mathrm{Q}\circ\mathrm{T}\circ\mathrm{N}$ 的函数值 $(p_1(s_1,\cdots,s_n),\cdots,p_m(s_1,\cdots,s_n))$，判断结果是否与原消息值 $m=(m_1,m_2,\cdots,m_m)$ 一致，相同即为合法，否则视为无效签名.

3　新方案的分析

3.1　新方案具备的性质

①不可伪造性：由于多变量公钥加密问题的难解性是 NP-C 问题，任何人无法根据公钥 $P=\mathrm{U}\circ\mathrm{Q}\circ\mathrm{T}\circ\mathrm{N}$ 计算出群签名成员的签名私钥 $\mathrm{T}_1,\mathrm{T}_2,\cdots,\mathrm{T}_n$. 签名成员的签名私钥是唯一的且由素矩阵组成的仿射变换，由定理 2.2 可知，签名私钥合成后的分解也是 NP-C 问题. 因此除了合法的签名成员以外，任何人都得不到也不能伪造出群签名成员的签名私钥，更无法伪造出群签名.

②群签名的可跟踪性：由于 n 名群签名成员 $\mathrm{A}_1,\mathrm{A}_2,\cdots,\mathrm{A}_n$ 的签名私钥 $\mathrm{T}_1,\mathrm{T}_2,\cdots,\mathrm{T}_n$ 是由素矩阵组成的仿射变换，由推论 2.1 可知，签名私钥 $\mathrm{T}_1,\mathrm{T}_2,\cdots,\mathrm{T}_n$ 合成的映射 T 只能由这 n 个签名私钥合

成，替换任何一个或若干个签名私钥，都无法合成映射 T，将导致签名失败. 因此，n 名群签名成员 A_1，A_2，…，A_n 与他们的签名私钥 T_1，T_2，…，T_n 是一一对应的，从而可以根据签名私钥追踪签名者，实现对群签名者的事后监督功能.

③群签名成员的可区分：由于不同的群签名成员的签名密钥是不同的，并且每个群签名成员与他们的签名密钥是一一对应的，因此群签名成员都是可以根据对应的签名私钥来区分的.

④不可抵赖性：任何群签名成员一旦参与签名，合成的映射 T 中就会含有该成员的私钥. 而群签名中每名成员的私钥都是与其一一对应的，且只有他本人知道，因此，群签名成员一旦作出签名后就不能否认.

⑤群签名成员的可注销性：如果临时需要撤销群签名成员 A_j 的签名权，那么成员 A_j 的签名私钥 T_j 将被删除，重新计算群签名成员签名私钥的合成 $T=T_1 \cdot T_2 \cdot \cdots \cdot T_{j-1} \cdot T_{j+1} \cdot \cdots \cdot T_n$ 以及公钥 $P=U \circ Q \circ T \circ N$，并公开公钥 P. 若当成员 A_j 仍继续签名时，产生的私钥的合成 T 是不合法的，因而用公钥 P 进行验证时将会出现验证失败. 因此只有当没有 A_j 签名时，才会签名成功，从而达到了注销群成员的签名权的目的.

3.2 新方案的安全性

由于多变量公钥加密问题的难解性是 NP-C 问题，本方案是在多变量公钥密码体制签名模型上增加了群签名成员的私钥，因此本方案继承了多变量公钥密码体制的安全性. 而这 n 个私钥 T_1，T_2，…，T_n 均为素矩阵仿射变换. 由定理 2.2 可知，当 T_1，T_2，…，T_n 合成仿射变换 $T=T_1 \cdot T_2 \cdot \cdots \cdot T_n$ 后，分解出 T_1，T_2，…，T_n 是 NP-C 问题. 从而，该方案在多变量签名体制困难问题的基础上，增加了大数分解的困难问题，因此大大增加了该方案的安全性.

3.3 抗合谋攻击性

由推论 2.1 可知，全体群签名成员私钥的合成映射 $T=T_1 \cdot T_2 \cdot \cdots \cdot T_n$ 的分解是唯一的，且只能是 T_1，T_2，…，T_n，即映射 T 只能由 T_1，T_2，…，T_n 合成. 也就是说全体群签名成员的私钥是唯一的，若干个私钥的合成也是唯一的，若替换任何一个或若干私钥，都无法合成映射 T，从而得到的签名值将被验证失败. 因此当合谋攻击者发动合谋攻击时，无法找到合法的私钥来替换他们现有的私钥进行签名，一旦有任何一个群签名成员替换了原始的私钥，签名将不成功. 因此本方案可以根据签名的私钥追踪签名者，并且避免了合谋攻击.

4 结论

本文提出了一种基于多变量公钥密码体制的群签名方案，在传统多变量签名体制基础上增加了 n 个群签名成员私钥的合成. 本文提出的新方案能从根本上抵抗合谋攻击和伪造签名攻击，而且能够真正实现签名成员身份的可追查性. 此外，新方案不仅继承了多变量公钥密码体制的安全性，还增加了大数分解的困难性，因此大大提高了方案的安全性. 因此该方案继承了多变量公钥密码体制的安全性，能抵抗量子计算机的破解，也具有群签名必要的基本性质，是后量子时代值得参考和应用的一种群签名体制.

参考文献(References)

[1] Chaum D, Heyst E V. Group signatures [C]// Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques. New York: Springer-Verlag, 1991: 257-265.

[2] Camenish J, Stadler M. Efficient group signatures for large group[J]. Lecture Notes in Computer Science, 1997, 1 294: 410-424.

[3] Camenish J, Michels M. A Group Signature Schemes Based on RSA-Variant [R]. BRICS, University of Aarhus, 1998: Technical Report Rs-98-27.

[4] Ateniese G, Camenisch J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme[J]. Lecture Notes in Computer Science, 2000, 1880: 255-270.

[5] Kim H J, Lm J I, Lee D H. Efficient and secure member deletion in group signature schemes [J]. Lecture Notes in Computer Science, 2001, 2015: 150-161.

[6] Li C M, Hwang T, Lee N Y. Remark on the threshold RSA signature scheme [J]. Lecture Notes in Computer Science, 1994, 773: 413-420.

[7] Sun Huihui, Chen Shaozhen. An efficient forward secure group signature scheme with revocation [J]. Journal of Electronics(China), 2008, 25(6): 798-802.

[8] Wang Zhanjun, Ma Haiying. Security analysis of a dynamic group signature scheme [J]. Computer Applications and Software, 2009, 26(7): 281-283.
王占君，马海英. 对一种动态群签名方案的安全性分析[J]. 计算机应用与软件，2009，26(7)：281-283.