文章编号：2095-2163(2023)06-0090-08 中图分类号：TP305 文献标志码：A

基于中国剩余定理的门限可传递签名方案

金 琳[1]，弓晓锋[2]
（1 贵州大学 计算机科学与技术学院，贵阳 550025；2 贵州省科技信息中心，贵阳 550025）

摘 要：针对现有可传递签名方案不满足门限应用需求的问题，提出一种门限可传递签名方案。首先，利用中国剩余定理构造 (t,n) 门限签名算法，实现只有参与签名的群组成员不少于指定的阈值时，才能生成有效的门限签名。其次，结合门限签名、ELGamal 同态和节点签名范例，构造安全可靠的可传递签名方案。一个或者多个签名者可以在不知道中间方私钥的条件下，对合成边签名进行认证，实现有向图结构中的门限签名可传递认证，从而提高签名认证效率。最后，通过安全性分析表明，该方案在随机预言机模型下，满足门限下的 CMA 安全，在保护隐私安全的同时，抵抗伪造签名攻击。

关键词：可传递签名；中国剩余定理；门限签名；CMA

Threshold transitive signature scheme based on Chinese remainder theorem

JIN Lin[1], GONG Xiaofeng[2]
(1 College of Computer Science and Technology, Guizhou University, Guiyang 550025, China;
2 Guizhou Science and Technology Information Center, Guiyang 550025, China)

【Abstract】 Aiming at the problem that the existing transitive signature schemes do not meet the requirements of threshold applications, a threshold transitive signature scheme is proposed. First, the Chinese remainder theorem is used to construct a (t,n) threshold signature algorithm which realizes that only when the group members participating in the signature are not less than the specified threshold, a valid threshold signature can be generated. Secondly, combining threshold signature, ELGamal homomorphism and node signature paradigm, a safe and reliable transitive signature scheme is constructed where one or more signers can be authenticated without knowing the private key of the intermediate party. It realizes the threshold transitive signature in the directed graph structure and improves the efficiency of signature authentication. Finally, the security analysis shows that under the random oracle model, the scheme satisfies the CMA security under the threshold, and can protect privacy security while resisting signature forgery attacks.

【Key words】 transitive signature; Chinese remainder theorem; threshold signature; CMA

0 引 言

DESMED[1]最早提出了 (t,n) 门限方案，实现只有参与签名的成员不少于指定的阈值 t 时，才能生成有效的群签名；之后，DESMED[2]又提出了一种基于 RSA 的 (t,n) 门限签名方案。SHAMIR[3]提出了基于 Lagrang 插值多项式的门限签名方案。之后，越来越多的门限签名方案被相继提出，并被广泛应用于实际生活场景中。但在一些特殊的应用环境中，门限签名的签名效率并不理想。例如，在分级诊疗系统中，如果上级医院 A 向下级医院 B 发送患者转诊请求，医院 B 接收到患者转诊数据时，则上级医院 A 需要向下级医院 B 证明患者转诊单的有效性及医院 A 身份的准确性，即上级医院 A 必须提供由权威机构 T 生成的签名，以证明医院 A 身份的真实性，确保转诊数据的真实性和完整性。此外，在 PKI 中的证书链及电子商务信息传递中也有类似的情况。在这些场景下，传统签名认证算法需要对等

基金项目：国家重点研发计划项目(2021YFB3101100)；国家自然科学基金联合基金重点支持项目(U1836205)；贵州省高层次创新型人才项目(黔科合平台人才[2020]6008)；贵阳市科技计划项目(筑科合[2021]1-5)；贵州省科技计划项目(黔科合平台人才[2020]5017)；贵州省科技计划项目(黔科合支撑[2022]一般 065)。

作者简介：金 琳(1997-)，女，硕士研究生，主要研究方向：密码学安全、属性加密、区块链；弓晓锋(1986-)，男，博士，教授，硕士生导师，主要研究方向：密码学、信息安全。

通讯作者：弓晓锋 Email：2289076883@qq.com

收稿日期：2022-05-26

级下的多个签名依次进行认证，计算花销大且认证效率低。

2002 年，Micali 等[4]提出了第一个可传递签名方案 MRTS，并将可传递签名的概念形式化。Bellare 等[5]提出了“节点签名范例”，并分别基于大整数因式分解和 RSA 困难性问题，构造了两种可传递签名方案。Van Heijist 等[6]提出了一种无向传递签名方案，通过安全性分析证明其无向传递签名可以通过“失败-停止”签名方案来实现。Yi[7]指出了有向树结构中的有向传递签名方案（DTS-HK），不能抵抗伪造攻击的问题。Zhou[8]提出了一种基于因式分解和强 RSA 的特定传递签名方案，并证明该传递签名方案在自适应选择消息攻击下，满足传递不可伪造性。Zhu[9]通过引入节点签名和边签名算法，提出了一种具体的无向传递签名方案，在传递图上定义的签名算法由单独的顶点签名算法和边签名算法组成，这两种算法可以共享传递图的状态信息。马春光等[10]提出了两种无状态图结构下的无向可传递签名方案，以解决传统具有状态的传递签名方案的计算效率问题。Neven[11]提出了一种基于有向树困难问题的简单高效的可传递签名方案，证明其安全性不依赖任何与 RSA 相关的安全假设。沈忠华等[12]提出了一种基于中国剩余定理的 (t,n) 有向门限签名方案。Peng 等[13]提出了一种通用可传递签名方案，实现双线性对、离散对数等困难问题下的可传递签名通用框架。Zhang 等[14]提出了具有方向状态函数的传递签名方案，并证明了所提方案在自适应 CMA 下是安全的。Zhu 等[15]提出了一种通用指定的多验证器传递签名方案，允许传递签名持有者将签名指定给多重验证者。Lin 等[16]提出了一种用于无向图的无状态传递签名（TS），并在随机预言机模型中的 M2SDH 假设下，证明该方案对自适应选择消息攻击具有传递不可伪造性。Geontae 等[17]提出了第一个基于格的无向图传递签名方案，并证明其方案在随机预言模型中是安全的。之后，Geontae 等[18]提出第一个格下的基于身份的传递签名方案。

可传递签名允许签名者验证图中边的合法性，即任何人给定公钥和邻边 (v_i,v_j)、边 (v_j,v_k) 上的两个签名，都可以计算边 (v_i,v_k) 上的第三个签名，能够提高签名的效率性及安全性，但上述可传递签名方案均不适用于群体决策场景中，无法做到门限签名传递。本文设计了一种基于中国剩余定理的门限签名算法，结合门限签名算法、ELGamal 同态加密和节点签名范例构造有向图下的可传递签名方案，实现门限签名的可传递认证，提高签名效率。并在 EUF-TS-CMA 安全模型下，证明本文所提方案是 CMA 安全的，能够在保护隐私安全的同时，抵抗伪造签名攻击。

1　基础知识

1.1　ElGamal 加密算法

ElGamal 加密算法是一种具有乘法同态的公钥加密系统。乘法同态加密能够直接通过密文相乘，得到相应的明文运算结果，而不需要对密文进行解密。具体算法如下：

$KeyGen(1^k)$ 密钥生成算法：输入安全参数 k，算法输出公私钥对 (pk,sk)。令 G 是阶为 q 的循环群，g 为 G 的生成元，随机选择整数 $x(1 \leqslant x \leqslant q-2)$，计算 $h = g^x \bmod q$，则公钥 $pk = (G,g,q,h)$，私钥 $sk = x$（保密）。

$Enc(pk,m)$ 加密算法：输入公钥 pk 和明文 m，输出密文 C。随机选择整数 r，计算 $E(m) = (c_1,c_2) = (g^r \bmod q, mh^r \bmod q)$。

$Dec(sk,C)$ 解密算法：输入私钥 sk 和密文 C，算法输出明文 m。计算可得 $m = c_2 \cdot c_1^{-x} \bmod q$。因其为乘法同态，则满足 $E(m_1) \times E(m_2) = E(m_1 \times m_2)$。

1.2　中国剩余定理

设 $m_1,m_2,\cdots,m_k$ 是两两互素的正整数，$M = \prod_{i=1}^{k} m_i$，则一次同余方程组

$$\begin{cases} x \equiv a_1 (\bmod m_1) \\ x \equiv a_2 (\bmod m_2) \\ \quad \cdots \\ x \equiv a_k (\bmod m_k) \end{cases}$$

对模 M 有唯一解：$x \equiv \left(\frac{M}{m_1}e_1a_1 + \frac{M}{m_2}e_2a_2 + \cdots + \frac{M}{m_k}e_ka_k\right) (\bmod M)$。

其中，e_i 满足 $\frac{M}{m_i}e_i \equiv 1 (\bmod m_i)(i = 1,2,\cdots,k)$。

1.3　可传递签名

可传递签名方案由一个算法组 $(TKG,TSig,TVer,Comp)$ 和 4 个集合 (K_S,K_P,M,S) 组成。其中，K_S 是私钥空间；K_P 是公钥空间；M 是消息空间；S 是签名空间。算法描述如下：

$TKG(1^k)$ 密钥生成算法：输入安全参数 k，算法输出公私钥对 (tpk,tsk)。

$TSig(tsk,m)$ 签名算法:输入私钥 tsk 和待签名消息 m, 算法输出签名 σ。对具有可传递二元关系的边和节点进行签名。

$TVer(tpk,m,\sigma)$ 验证算法:输入公钥 tpk、被签名信息 m 和签名 σ。如果 σ 是信息 m 的有效签名,算法输出 1,否则输出 0。

$Comp(tpk;m_1,m_2;\sigma_1,\sigma_2)$ 签名合成算法:输入公钥 tpk 和被签名信息 m_1、m_2, 以及签名 σ_1、σ_2。如果 σ_1 和 σ_2 是有效签名,则算法输出合成签名 σ,否则输出 $\perp$。将具有传递关系的两个边签名合成为一个新的边签名。

可传递签名的传递性可描述为:已知 m_1 和 m_2 的签名为 σ_1 和 σ_2, 如果 $m_1 \oplus m_2 = m$, 则任何人都可以调用合成算法 $Comp$ 生成一个新的签名 $\sigma = Comp(tpk;m_1,m_2;\sigma_1,\sigma_2)$, 并且满足 $TVer(tpk,m,\sigma)=1$。

2 安全模型

门限可传递签名方案(Threshold Transitive Signature Scheme,TTSS)的安全模型是适应性选择门限签名和选择消息攻击下,具有存在性不可伪造性(existential unforgeability against adaptive chosen threshold signature and chosen messages attacks,EUF-TS-CMA)游戏。游戏中包含一个挑战者和一个敌手,挑战者模拟系统运行并回答敌手的询问。具体游戏过程如下:

(1)系统建立:挑战者运行系统初始化算法 $Setup(1^\kappa)$, 将生成的公钥 tpk 和 群公钥 y_U 发送给敌手 A;

(2)签名询问:敌手 A 可以向挑战者多项式有界次适应性询问边 (v_i,v_j) 的签名,挑战者向 A 返回 (v_i,v_j) 的合法签名 $\sigma_{i,j}$;

(3)挑战阶段:敌手 A 伪造签名 $GS'=\{S',W,R,m\}$,挑战者计算 $u'=(g^{S'}(y_U)^R W)\bmod p$ 和 $Z'=u'^{x_B}\bmod p$ 来验证等式 $R=h(Z',W,m)\bmod q$ 是否成立;敌手 A 伪造边签名 $\sigma_{\tau,i}\leftarrow A_1^{O_{TS},O_C,O_{TV}}(v_\tau,v_i)$, 挑战者运行 $TSig$ 和 $Comp$ 对其边进行签名计算。

(4)当且仅当 $TVer(tpk,(v_i,v_k),\sigma_{i,k})\neq\perp$ 且 $b=b'$ 时,游戏输出"1";否则游戏输出"0"。

为便于理解,具体的形式化定义如实验 1 所示:

实验 1 $\mathrm{Exp}_{TTSS,A}^{TS-CMA}(1^\kappa)$

输入 安全参数 κ

输出 "0"或"1"

1 $((tpk,tsk),(x_U,y_U))\leftarrow Setup(1^\kappa)$

2 $((l_i,\Sigma_i),(l_j,\Sigma_j),\sigma_{i,j})\leftarrow TSig(tsk,(v_i,v_j))$

3 $\sigma_{i,k}\leftarrow Comp((v_i,v_j),(v_j,v_k);\sigma_{i,j},\sigma_{j,k})$

4 $\sigma_{\tau,i}\leftarrow A_1^{O_{TS},O_C,O_{TV}}(v_\tau,v_i)$

5 $b\leftarrow\{0,1\}$

6 if $b=1$

7 then $\sigma_{i,k}\leftarrow TSig(tsk,(v_i,v_k))$

8 else

9 $\sigma_{i,k}\leftarrow Comp((v_i,v_j),(v_j,v_k);\sigma_{i,j},\sigma_{j,k})$

10 $b'\leftarrow A_2^{O_{TS},O_C}((v_i,v_j),(v_j,v_k),\sigma_b)$

11 如果 $TVer(tpk,(v_i,v_k),\sigma_{i,k})\neq\perp$ 并且 $b=b'$ 返回"1";否则返回"0"

定义 1 如果对于任意的 PPT 敌手 A 在以上安全模型中输出"1"的概率是可忽略的,即 $\Pr[\mathrm{Exp}_{TTSS,A}^{TS-CMA}(1^\kappa)=1]\leqslant\varepsilon$($\varepsilon$ 为一个可忽略的概率阈值),则门限可传递签名方案是安全的(CMA)。

3 方案描述

设:U 是 n 个用户的集合,H 是 U 的子集,H 包含 t 个用户,有一个可信秘密共享中心(Share Distribution Center,SDC),来生成公共参数和秘密共享。如果 H 中的用户希望为用户 B 签署消息 m, 则预先约定一个可信任的群签名生成中心(Designated Combiner,DC),收集 H 中所有成员的部分签名,以生成有效群签名。在有向图结构中,每个节点可以看作一个独立的机构,每个机构有自己的群签名,将群签名作为节点签名的一部分,参与可传递签名算法。在门限传递签名算法中,当接受者对群签名认证时,只需验证一次,且签名者可以使用边 (v_{i-1},v_i) 和 (v_i,v_{i+1}) 上的两个签名,对边 (v_{i-1},v_{i+1}) 进行签名,在不知道对方私钥的情况下,实现门限签名的可传递。如图 1 所示。

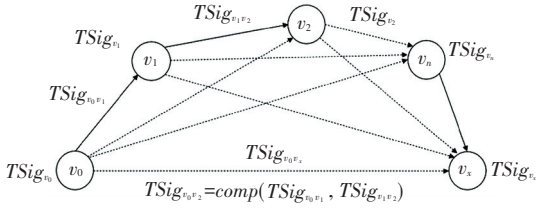

图 1 可传递签名

Fig. 1 Transitive signature

门限可传递签名方案(TTSS)算法描述如下:

(1) $Setup(1^\kappa)\rightarrow((tpk,tsk),(x_U,y_U))$:系统初始化算法,由秘密共享中心 SDC 运行,用以确定系统参数、群签名的公私钥对 (x_U,y_U) 及传递签名的公私钥对 (tpk,tsk)。

其中，pk 为同态加密公钥；spk 为签名中心的签名公钥；sk 为同态加密私钥；ssk 为签名中心的签名私钥。公钥 $tpk=(pk,spk)$ 对外公开，私钥 $tsk=(sk,ssk)$ 保密。算法描述如下：

Setup 算法

输入　安全参数 1^{κ}

输出　密钥对 (tpk,tsk) 和 (x_U,y_U)

1 计算 $(pk,sk)\leftarrow KeyGen(1^k)$

2 $(spk,ssk)\leftarrow Key(1^k)$

3 SDC 选取整数 a（保密）和 g（公开）

4 选择素数 p,q 及 n 个整数 $d_1,d_2,\cdots,d_n$，

5 其中 $p>a$

6 $d_1<d_2<\ldots<d_n$

7 对任意的 $i,\gcd(d_i,p)=1$

8 对 $i\neq j,\gcd(d_i,d_j)=1$

9 $d_1d_2\cdots d_t>p\,d_n\,d_{n-1}\cdots d_{n-t+2}$

10 计算 $D=d_1d_2\cdots d_t$，即为 $d_1,d_2,\cdots,d_n$ 中最小的 t 个 d_i 的积

11 选取随机整数 $\lambda,\lambda\in Z_{[D/p]}$，计算 $a'=a+\lambda p$，$a'\in Z_D$

12 设 $x_U=a\bmod p$ 为 U 的群密钥，则 SDC 计算群公钥 $y_U=g^{x_U}\bmod q$

13 SDC 为 U 中每个用户计算共享秘密 $a_i(i=1,2,\cdots,n)$，$a_i=a'\bmod d_i$，$i=1,2,\cdots,n$

14 SDC 通过安全信道将 (a_i,d_i) 发送至每个成员，a_i 作为每个成员 i 的私钥

（2）$SignGen(K_{i_1},K_{i_2})\rightarrow s_{j_i}$：部分签名生成算法，由群签名成员运行该算法，通过各自拥有的共享秘密 (a_{j_t},d_{j_t})，生成对应 t 个成员各自的部分签名 s_{j_i}。算法描述如下：

SignGen 算法

输入　整数 $K_{i_1},K_{i_2}\in Z_P$

输出　部分签名 s_{j_i}

1 假设 U 中的 t 个成员（$U_{j_1},U_{j_2},\cdots,U_{j_t}$ 构成集合 H）同意为用户 B 对消息 m 进行签名，其分别拥有共享秘密 $(a_{j_1},d_{j_1}),(a_{j_2},d_{j_2}),\cdots,(a_{j_t},d_{j_t})$

2 用户 B 选择自己的密钥 x_B，然后计算 $y_B=g^{x_B}\bmod q$，并将 y_B 对 H 中的所有成员公开

3 每个成员 U_{j_i} 随机选择 $K_{i_1},K_{i_2}\in Z_P$

4 计算 $w_{j_i}=g^{K_{i_2}-K_{i_1}}\bmod q,z_{j_i}=y_B{}^{K_{i_2}}\bmod q$，将 w_{j_i} 公开，z_{j_i} 作为 H 中所有成员秘密共享

5 每个成员计算 $W=\prod_{i\in H}w_{j_i}\bmod q$，$Z=\prod_{i\in H}z_{j_i}\bmod q$

6 计算 $R=h(Z,W,m)\bmod p$

7 所有成员 U_{j_i} 在 H 范围内公开 d_{j_i}，H 中每个成员都计算 $D_1=d_{j_1}d_{j_1}\ldots d_{j_t}$

8 计算 $\delta_{j_i}=\dfrac{D_1}{d_{j_i}}$，其中 δ'_{j_i} 满足 $\delta'_{j_i}\delta_{j_i}=1\bmod d_{j_i}$，$i=1,2,\cdots,t$；

9 每个成员计算 $KS_{j_i}=a_{j_i}\delta'_{j_i}\delta_{j_i}\bmod D_1$，$i=1,2,\cdots,t$

10 随机选取整数 K_{i_1}

11 计算各自的部分签名 $s_{j_i}=(K_{i_1}-KS_{j_i}\circ R)\bmod D_1$

12 所有成员完成各自的部分签名后，都将其发送给群签名生成中心 DC

（3）$GSignGen(s_{j_i})\rightarrow GS$：群签名生成算法，由 DC 运行，通过中国剩余定理生成群签名 GS，并将其发送给用户 B，用户 B 可以用自己的私钥 x_B 判定群签名的有效性。算法描述如下：

GSignGen 算法

输入　t 个成员的部分签名 s_{j_i}

输出　群签名 GS

1 DC 收到 t 个成员的部分签名 s_{j_i} 后，生成群签名 $GS=\{S,W,R,m\}$，其中 $S=\sum_{i=1}^{t}s_{j_i}\bmod p$

2 将 GS 发送给用户 B

3　B 收到 DC 的群签名 GS 后计算 $u=(g^S(y_C)^R W)\bmod q,Z=u^{x_B}\bmod q$

4 $R'=h(Z,W,m)\bmod p$

5 若 $R'=R$，证明生成的群签名有效

（4）$TSig(tsk,(v_i,v_j),GS_i,GS_j)\rightarrow((l_i,\Sigma_i),(l_j,\Sigma_j),\sigma_{i,j})$：传递签名生成算法，通过计算生成节点签名和边签名。其中，Enc 为同态加密算法，Sig 为标准签名算法，ϕ 为同态映射。算法描述如下：

TSig 算法

输入　传递签名私钥 tsk，节点 v_i,v_j，群签名 GS_i,GS_j

输出　边签名 $\sigma_{i,j}$

1 算法检测 $v_i,v_j\in V$，如果 $v_i\notin V$，则操作如下：

2 将节点 v_i 加入到 V 中，随机选择 $l_i\in Z_N^*$ 为节点 v_i 的私有标签

3 计算 $pl_i=Enc(pk,l_i)$ 作为节点 v_i 的公共标签

4 计算节点 v_i 的标准签名 $\sigma_i=Sig(ssk,v_i\parallel pl_i)$

5 生成节点 v_i 的证书 $\Sigma_i=(v_i,pl_i,GS_i,\sigma_i)$

6 同理,如果 $v_j\notin V$,则将节点 v_j 加入到 V 中,为其生成私有标签 l_j、公共标签 pl_j 及其证书 $\Sigma_j=(v_j,pl_j,GS_j,\sigma_j)$

7 输出边 (v_i,v_j) 的签名 $\sigma_{i,j}=(\Sigma_i,\Sigma_j,\delta_{i,j})$,其中 $\delta_{i,j}=\phi(l_i,l_j)=l_i\circ l_j^{-1}$

(5) $Comp((v_i,v_j),(v_j,v_k);\sigma_{i,j},\sigma_{j,k})\rightarrow\sigma_{i,k}$:边签名合成算法,输入边 (v_i,v_j) 的签名 $\sigma_{i,j}$ 和边 (v_j,v_k) 的签名 $\sigma_{j,k}$。其中,边 (v_i,v_j) 和边 (v_j,v_k) 是具有传递关系的两条边。算法描述如下:

Comp 算法

输入 边 $(v_i,v_j),(v_j,v_k)$ 及边签名 $\sigma_{i,j},\sigma_{j,k}$

输出 合成边签名 $\sigma_{i,k}$

1 计算 $\delta_{i,k}=\phi(l_i,l_k)=\phi(l_i,l_j)\circ\phi(l_j,l_k)=\delta_{i,j}\circ\delta_{j,k}$

2 $\sigma_{i,k}=(\Sigma_i,\Sigma_k,\delta_{i,k})$

3 即 $Comp((v_i,v_j),(v_j,v_k);\sigma_{i,j},\sigma_{j,k})\rightarrow\sigma_{i,k}$

(6) $TVer(tpk,(v_i,v_j),\sigma_{i,j})\rightarrow\{0,1\}$:签名验证算法,输入 tpk,节点 v_i、v_j 及边签名 $\sigma_{i,j}$,用来验证节点签名及边签名的合法性。算法描述如下:

TVer 算法

输入 公钥 tpk,节点 v_i,v_j 及边签名 $\sigma_{i,j}$

输出 "1"或"0"

1 验证节点 v_i,v_j 的证书 Σ_i 和 Σ_j 的合法性

2 验证 $Enc(pk,\delta_{i,j})=Enc(pk,l_i)*Enc(pk,l_j^{-1})=Enc(pk,l_i\circ l_j^{-1})$ 是否成立

3 其中,$l_i\circ l_j^{-1}=\phi(l_i,l_j)$

4 若以上验证都通过,则算法输出"1",否则输出"0"

5 即 $TVer(tpk,(v_i,v_j),\sigma_{i,j})\rightarrow\{0,1\}$

其中,$HE=(KeyGen,Enc,Dec)$ 为 IND-CPA 安全的同态加密方案,$SG=(Key,Sig,Ver)$ 是 CMA 安全的标准签名方案,消息运算符记为"$\circ$",密文运算符记为"$*$",消息 x 的逆为 x^{-1}。

4 方案分析

4.1 正确性分析

由于 t 个成员 $U_{j_1},U_{j_2},\cdots,U_{j_t}$ 分别拥有共享秘密 $(a_{j_1},d_{j_1}),(a_{j_2},d_{j_2}),\cdots,(a_{j_t},d_{j_t})$,且满足以下同余式:

$$\begin{cases}x\equiv a_{j_1}(\mathrm{mod}d_{j_1})\\x\equiv a_{j_2}(\mathrm{mod}d_{j_2})\\\cdots\\x\equiv a_{j_t}(\mathrm{mod}d_{j_t})\end{cases}$$

已知 $\gcd(d_{j_i},d_{j_k})=1,j_i\neq j_k$,根据中国剩余定理可知,同余方程有唯一解 $x\equiv\sum_{i=1}^{t}a_{j_i}\delta'_{j_i}\delta_{j_i}(\mathrm{mod}D_1)$。

其中,$D_1=d_{j_1}d_{j_1}\cdots d_{j_t}$,$\delta_{j_i}=\dfrac{D_1}{d_{j_i}}$,$\delta'_{j_i}\delta_{j_i}=1\mathrm{mod}d_{j_i}$,$i,k=1,2,\cdots,t$。因 $D=d_1d_2...d_t$ 为最小的 t 个 $d_i(i=1,2,\cdots,n)$ 的乘积,故 $D_1\geqslant D$,能在模 D 的范围内唯一确定 a',即 $a'=x\mathrm{mod}D$。而 $a'=a+\lambda p$,则 $a'=a\mathrm{mod}\,p$。又因 $p>a$,故

$$S=\sum_{i=1}^{t}s_{j_i}\mathrm{mod}p=\Big[\sum_{i=1}^{t}(K_{i_1}-KS_{j_i}\circ R)\mathrm{mod}D_1\Big]\mathrm{mod}p=$$

$$\Big[\sum_{i=1}^{t}K_{i_1}-R\sum_{i=1}^{t}KS_{j_i}\mathrm{mod}D_1\Big]\mathrm{mod}p=$$

$$\Big[\sum_{i=1}^{t}K_{i_1}-R\sum_{i=1}^{t}a_{j_i}\delta'_{j_i}\delta_{j_i}\mathrm{mod}D_1\Big]\mathrm{mod}p=$$

$$\sum_{i=1}^{t}K_{i_1}-Ra\mathrm{mod}p$$

则

$$u=(g^S(y_U)^RW)\mathrm{mod}q=g^{\sum_{i=1}^{t}K_{i_1}-Ra\mathrm{mod}p}g^{Rx_U}W\mathrm{mod}q=$$

$$g^{\sum_{i=1}^{t}K_{i_1}-Ra\mathrm{mod}p}g^{Ra\mathrm{mod}p}\prod_{i=1}^{t}g^{K_{i_2}-K_{i_1}}\mathrm{mod}q=$$

$$\prod_{i=1}^{t}g^{K_{i_2}}\mathrm{mod}q$$

故

$$u^{x_B}=\prod_{i=1}^{t}g^{x_BK_{i_2}}\mathrm{mod}q=\prod_{i=1}^{t}y_B^{K_{i_2}}\mathrm{mod}q=Z\mathrm{mod}q$$,因此 $R=h(Z,W,m)\mathrm{mod}p$。

4.2 安全性分析

定理 1 若 DLP 是困难的,则该方案具有隐私保护性。

证明 已知 $y_U=g^{x_U}\mathrm{mod}q$,若敌手 A 想要通过群公钥 y_U 来获取群密钥 x_U,其难度相当于求解离散对数,而且敌手 A 想要通过 d_i 来获取每个成员的密钥 a_i 是不可能的。因为 $a_i\equiv a'\mathrm{mod}d_i$,在此同余方程中 a' 为 SDC 秘密保留,故只通过 d_i 想要从同余方程 $a_i\equiv a'\mathrm{mod}d_i$ 中解得 a_i 是不可能的。在部分签名的生成阶段,敌手 A 不可能获取整数 K_{i_1}、共享密钥 a_i 和部分签名 s_{j_i}。因为 $s_{j_i}=(K_{i_1}-KS_{j_i}\circ R)\mathrm{mod}D_1$,其中 $KS_{j_i}=a_{j_i}\delta'_{j_i}\delta_{j_i}\mathrm{mod}D_1$,敌手 A 无法得到 s_{j_i}、K_{i_1} 和 a_i,故无法确定同余方程的解。在群签名产生过程中,群签名中心 DC 只知道每个成员的部分签名 s_{j_i},则敌手 A 不可能通过同余式 $s_{j_i}=(K_{i_1}-KS_{j_i}\circ R)\mathrm{mod}D_1$ 获得 a_i 和 x_U 等其他信息。

综上,该方案具有隐私保护性。

定理 2　若门限可传递签名方案 EUF-TS-CMA 安全，则该方案可以抵抗伪造签名攻击。

证明　根据门限可传递签名算法满足 EUF-TS-CMA 可知，即便多项式时间敌手 A 伪造签名 $GS' = \{S', W, R, m\}$ 给用户 B，用户 B 可以通过计算 $u' = (g^{S'}(y_U)^R W) \bmod p$ 和 $Z' = u'^{x_B} \bmod p$ 来验证等式 $R = h(Z', W, m) \bmod q$ 是否成立，来判断签名的真实性。故敌手 A 不能为自己选定的消息伪造一个合法的签名，故该方案能够抵抗伪造签名攻击。

定理 3　少于 t 个成员是无法获知系统的关键参数 a'，进而敌手 A 无法知道群密钥。

证明　假设敌手 A 知道 $t-1$ 个成员的共享秘密 $(a_{j_1}, d_{j_1}), (a_{j_2}, d_{j_2}), \cdots, (a_{j_{t-1}}, d_{j_{t-1}})$，就可能知道 a' 关于模 $D_2 = d_{j_1} d_{j_2} \ldots d_{j_{t-1}}$ 有唯一解 x。但由于 $D = d_1 d_2 \cdots d_t$ 为最小的 t 个 d_i 的乘积，所以 D/p 大于任意一个 $t-1$ 个 d_i 之积，因此 $D/D_2 > p$，又 $\gcd(p, D_2) = 1$，使得 $x \leqslant D$ 和 $x \equiv a' \bmod D_2$ 的整数 a' 在模 p 的所有同余类上均匀地分布，故敌手 A 就无法获得足够的信息去确定 a'，进而无法确定群密钥 x_U。

定理 4　若方案 TTSS 是 CMA 安全性的，当且仅当同态加密方案是 IND-CPA 安全的，且签名方案 SG 是适应性 CMA 安全的。

证明　在方案攻击实验中，允许任意 PPT 敌手 A 选择任意消息的请求，其在多项式时间内产生与现有有效签名不同签名的概率可以忽略不计，即敌手 A 的攻击优势是可忽略的，其成功率为

$$\Pr[(A^{TSig(\kappa,)} = (v_\tau, \Sigma'_\tau, \sigma'_{\tau,\kappa})) \wedge v_\tau \notin V \wedge (TVer(tpk, v_\tau, \Sigma_\tau, \sigma_{\tau,\kappa}) = 1) \wedge \sigma_{\tau,\kappa} \notin Span\{\sigma_{i,j}\}]$$

其中，$\{m_1, m_2, \cdots, m_n\}$ 为已签名消息集；κ 为安全参数；$A^{TSig(\kappa,)} = (m, \sigma_m)$ 表示敌手 A 把 $TSig$ 作为预言机访问产生签名 (m, σ_m)。

定义敌手在 CMA 安全性概念下攻破 TTSS 的成功率为：$Suc_{TTSS,A}^{TS-CMA}(1^\kappa) = \Pr[\mathrm{Exp}_{TTSS,A}^{TS-CMA}(1^\kappa) = 1]$；在 IND-CPA 安全性概念下攻破同态加密 HE 的优势为：$Adv_{HE,A}^{IND-CPA}(1^\kappa) = |2\Pr[\mathrm{Exp}_{HE,A}^{IND-CPA}(1^\kappa) = 1] - 1|$；在适应性 CMA 安全性概念下攻破 SG 的成功率为：$Suc_{SG,A}^{CMA}(1^\kappa) = \Pr[\mathrm{Exp}_{SG,A}^{CMA}(1^\kappa) = 1]$。

实验 2　$\mathrm{Exp}_{SG,A}^{CMA}(1^\kappa)$

输入　安全参数 κ

输出　“0”或“1”

1　$(tpk, tsk) \leftarrow Key(1^k)$

2　$\sum_\tau \leftarrow A_1^{O_S}(v_\tau)$

3 如果 $TVer(tpk, v_\tau, \sum_\tau) \neq \perp$ 返回“1”；否则返回“0”

实验 3　$\mathrm{Exp}_{HE,A}^{IND-CPA}(1^\kappa)$

输入　安全参数 κ

输出　“0”或“1”

1 $c \leftarrow A_1^{O_E}(m)$

2 $b \leftarrow \{0, 1\}$

3 $c_b \leftarrow Enc(pk, m_b)$

4 $b' \leftarrow A_1^{O_E}(sk, c_b, m_0, m_1)$

5 如果 $b = b'$ 返回“1”；否则返回“0”

采用反证法证明该安全性定理。首先假设 TTSS 满足 CMA 安全性，但 HE 不满足 CPA 安全性，且 SG 不满足 IND-CMA 安全性。构造算法 A 以不可忽略概率攻破方案 TTSS。

由于 HE 不满足 IND-CPA 安全性，则存在算法 A_1：$Adv_{HE,A_1}^{IND-CPA}(1^\kappa) > \varepsilon_1$（其中 ε_1 是不可忽略概率），即在实验 $\mathrm{Exp}_{SG,A}^{CMA}(1^\kappa)$ 中，A_1 以 ε_1 的概率区分 m_0 和 m_1。A_1 便以 ε_1 的概率获得节点 v_i 的私有标签 l_i，进而伪造出一个新节点 $v_\tau (v_\tau \notin V)$ 且满足 $(TVer(tpk, v_\tau, \Sigma_\tau, \sigma_{\tau,\kappa}) = 1)$，从而构造一个边签名 $\delta_{\tau,i} = \phi(l_\tau, l_i) = l_\tau \circ_i^{-1}$，显然 $\sigma_{\tau,i} \notin Span\{\sigma_{i,j}\}$。

由于 SG 不满足 CMA 安全性，则存在算法 A_2：$Suc_{SG,A_2}^{CMA}(1^\kappa) > \varepsilon_2$（其中 ε_2 是不可忽略概率），即在实验 $\mathrm{Exp}_{SG,A}^{CMA}(1^\kappa)$ 中，A_1 以 ε_2 的概率伪造出新节点 v_τ 的证书 Σ_τ。因此，算法 A_2 将以不可忽略的概率伪造出节点 v_τ 的证书 Σ_τ 和一个边签名 $\delta_{\tau,i}$。这样，算法 $A = (A_1, A_2)$ 攻破 TTSS 的成功率为

$$Suc_{TTSS,A}^{TS-CMA}(1^\kappa) > \varepsilon, \varepsilon = \min\{\varepsilon_1, \varepsilon_2\}$$

即 TTSS 不满足 CMA 安全，与假设矛盾。故方案 TTSS 满足 CMA 安全性一定有 HE 满足 CPA 安全性，且 SG 满足 IND-CMA 安全性。反之，假设 HE 满足 CPA 安全性，且 SG 满足 IND-CMA 安全性，但 TTSS 不满足 CMA 安全性。

由于 TTSS 不满足 CMA 安全，则存在一个敌手算法 A 在多项式时间内攻破 TTSS 的成功率不可忽略，即 $Suc_{TTSS,A}^{TS-CMA}(1^\kappa) > \varepsilon$（$\varepsilon$ 是不可忽略的概率）。

在实验 $\mathrm{Exp}_{TTSS,A}^{TS-CMA}(1^\kappa)$ 中，存在算法 S_1，至少以 ε 的概率区分出一个签名是通过 $TSig$ 算法生成的还是通过 $Comp$ 算法合成的，根据同态加密的性质：

$$\delta_{i,k} = \phi(l_i, l_k) = \phi(l_i, l_j) \circ \phi(l_j, l_k) = \delta_{i,j} \circ \delta_{j,k}$$

可知，若 $\sigma_{i,j}, \sigma_{j,k} \in Span\{\sigma_{i,j}\}$，则 $TSig(tsk, (v_i, v_k)) \rightarrow ((l_i, \Sigma_i), (l_k, \Sigma_k), \sigma_{i,k})$ 与 $Comp((v_i, v_j), (v_j, v_k); \sigma_{i,j}, \sigma_{j,k}) \rightarrow \sigma_{i,k}$ 是不可区分的。

在实验 $\mathrm{Exp}_{TTSS,A}^{TS-CMA}(1^\kappa)$ 中，存在算法 S_2，至少以 ε

的概率获得节点 v_k 的私有标签 l_k 和证书 Σ_k，即 A 要攻破公共标签 w_k 和证书 Σ_k，则 S_2 攻破 HE 的优势为 $Adv_{HE,S_2}^{IND-CPA}(1^\kappa) > \varepsilon$。这样，$S_2$ 就以 ε 的概率获得 v_k 的私有标签 l_k，并伪造出边 (v_τ, v_k) 的 $\sigma_{\tau,\kappa}$；同时，A 攻破 SG 的成功率为 $Suc_{SG,A}^{CMA}(1^\kappa) > \varepsilon$，则 S_2 至少以 ε 的概率伪造出自己的标准签名 σ_τ 和证书 Σ_τ。

故 HE 不满足 CPA 安全性，且 SG 不满足 IND-CMA 安全性，与假设矛盾。

综上所述，方案 TTSS 是 CMA 安全性的，当且仅当同态加密方案是 IND-CPA 安全的，且签名方案 SG 是适应性 CMA 安全的。

4.3 性能分析

将本文方案与方案 MRTS[4]、RSATS[14]在签名开销、验证开销、签名合成开销等方面进行分析比对，其结果见表 1。表 1 中，*ops* 为比特运算量；T_e 为一次求幂运算时间；*H.* 为同态加密算法；T_m 为一次求加/差/积运算时间；T_S. 为标准签名方案；T_p 为一次双线性对运算时间；G 为 q 阶有限群。

表 1 性能对比分析

Tab. 1 Performance comparison analysis

方案	签名开销	验证开销	签名合成开销
MRTS	$2T_S.signs.\&2T_e inG$	$2T_S.Verifs\&2T_e + 1T_m inG$	$2T_m inZ_q$
RSATS	$2T_S.signs.\&2T_e inZ_n^*$	$2T_S.Verifs\&1T_e inZ_n^*$	$O(\mid n \mid^2) ops$
TTSS	$2T_S.signs.\&2H.encs$	$2T_S.Verifs\&1H.enc$	$1T_m inZ_q$

根据表 1 可知，所提方案 TTSS 中，签名开销较之前没有明显降低，但签名验证开销和签名合成效率都有很大提高。总体上，本方案在性能方面具有一定优势。

5 结束语

在多签名场景中，传统签名认证需要对多个签名进行逐个认证，而且签名长度与签名者人数有关，计算花销大且认证效率低。针对以上问题，本文提出了一种门限可传递签名方案。通过引入中国剩余定理、ELGamal 公钥密码理论，并结合“节点签名范例”构造有向图结构下的 (t,n) 门限可传递签名方案，能够保护用户隐私安全的同时，抵抗伪造签名攻击，提高传递签名的算法效率，解决签名认证安全和效率问题。本方案在上下级群体决策中有较好的应用前景，如何将本方案更好地应用到分级诊疗系统中将是下一步的研究工作。

参考文献

[1] DESMEDT Y, FRANKEL Y. Society and group-oriented cryptography [C]// Advance in Cryptology-Crypto-87. New York: Springer-Verlag, 1988: 457-469.

[2] DESMEDT Y, FRANKEL Y. Shared generation of authenticators and signatures [C]// /Advances in Cryptology-Crypto-91. New York: Springer-Verlag, 1991: 457-469.

[3] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(4): 612-613.

[4] MICALI S, RIVEST R L. Transitive signature schemes [C]// Topics in Cryptology—CT-RSA 2002: The Cryptographers' Track at the RSA Conference 2002 San Jose, CA, USA, February 18-22, 2002 Proceedings. Springer Berlin Heidelberg, 2002: 236-243.

[5] BELLARE M, NEVEN G. Transitive signatures based on factoring and RSA[C]//Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1 - 5, 2002 Proceedings 8. Springer Berlin Heidelberg, 2002: 397-414.

[6] VAN HEIJST E, PEDERSEN T P, PFITZMANN B. New constructions of fail-stop signatures and lower bounds [C]// Advances in Cryptology—CRYPTO'92: 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16-20, 1992 Proceedings 12. Springer Berlin Heidelberg, 1993: 15-30.

[7] YI X, TAN C H, OKAMOTO E. Security of kuwakado-tanaka transitive signature scheme for directed trees [J]. IEICE Transactions on Fundamentals, 2004, E87-A (4): 955-957.

[8] SUJING Z. Transitive signatures based on non-adaptive standard signatures[J]. Cryptology ePrint Archive, 2004.

[9] ZHU H. Model for undirected transitive signatures [J]. IEEE Proceedings Communications, 2004, 151(4): 312-315.

[10] MA C, WU P, GU G. A new method for the design of stateless transitive signature schemes [C]//Advanced Web and Network Technologies, and Applications: APWeb 2006 International Workshops: XRA, IWSN, MEGA, and ICSE, Harbin, China, January 16-18, 2006. Proceedings 8. Springer Berlin Heidelberg, 2006: 897-904.

[11] NEVEN G. A simple transitive signature scheme for directed trees [J]. Theoretical Computer Science, 2008, 396(1-3): 277-282.

[12] 沈忠华. 基于中国剩余定理的(t,n)有向门限签名方案[J]. 浙江大学学报(理学版), 2010, 37(1): 42-45.

[13] PENG C H, TIAN Y L, ZHANG B, et al. General transitive signature scheme based on homomorphic encryption [J]. J. Commun, 2013, 34(11): 18-25.

[14] ZHANG Yichen, JIANG Yong, LI Jiguo. Provably secure directed transitive signature [J]. Computer Engineering and Applications, 2014, 50(19): 74-77.

(下转第 102 页)