一种基于 DAA 的强匿名性门限签名方案

甄鸿鹄[①②] 陈 越[①] 郭渊博[①]
[①](解放军信息工程大学电子技术学院 郑州 450004)
[②](解放军 63612 部队 瓜州 736100)

摘 要：针对目前大多数门限签名方案不能实现签名成员匿名或匿名效果比弱的问题，该文提出了一种带有子密钥分发中心的强匿名性(n, t)门限签名方案。方案主要基于可信计算组织在其 v1.2 标准中采用的直接匿名认证(Direct Anonymous Attestation, DAA)方案，以及零知识证明和 Feldman 门限秘密共享等技术实现。相较已有方案，该方案即使在签名验证者和子密钥分发中心串通的情况下，也能够实现子签名的不可追踪性，也即可确保子签名成员的强匿名性。分析显示，方案除具有强匿名性外还具备签名子密钥不可伪造、子签名可验证以及一定的鲁棒性等特征。该方案在“匿名表决”等一些对匿名性要求较高的场合中有着重大的应用价值。

关键词：门限签名；匿名表决；直接匿名认证(DAA)；零知识证明；秘密共享
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2010)03-0693-07
DOI:10.3724/SP.J.1146.2009.00287

A Strong Anonymity Threshold Signature Scheme Based on DAA

Zhen Hong-hu[①②] Chen Yue[①] Guo Yuan-bo[①]
[①](*Institute of Electronic Technology, the PLA Information Engineering University, Henan Zhengzhou* 450004, *China*)
[②](*PLA NO.* 63612 *Unit, Guazhou* 736100, *China*)

Abstract: For most present threshold signature schemes, sub-sign member can not sign a message anonymously or theirs anonymity is very weak. To improve their anonymity, a strong anonymity (n, t) threshold signature scheme based on DAA (Direct Anonymous Attestation), which is adopted by Trusted Computing Group v1.2 specifications, is proposed. Compared with the others, the scheme colligates DAA, zero-knowledge proof and Feldman verifiable secret sharing technique to achieve untraceable sub-sign and insure strong anonymity of signers, even the verifier and the dealer are colluded. Besides strong anonymity, analysis shows the scheme also has the property of unforgeable share, verifiable sub-sign, and robustness etc. It can be used in the situations which desire high-level anonymity such as “anonymous voting”.

Key words: Threshold signature; Anonymous voting; Direct Anonymous Attestation (DAA); Zero-knowledge proof; Secret sharing

1 引言

门限签名最早由Desmedt等人引进[1]，其需要多方共同参与来完成对消息的签名，因而可提高签名及认证的安全性与可靠性。在电子商务、电子政务中门限签名也有着广阔的应用，如企业、政府进行决策时，可将密钥分发给一个决策群体，然后由这个群体中的成员采用门限签名对其进行表决，也即当超过门限时，决议才会生效，这将有助于提高决策的科学性。故签名群组成员对消息m的一次门限签名在一定程度上就是对m进行了一次表决，但是在现实生活中，当人们对于诸如敏感的人事任命决议等进行表决时，却希望能够实现匿名的表决，也即不希望别人知道自己是否进行了签名(签名意味着赞同)，故一个能够保护签名者身份隐私的匿名门限签名方案将是非常有意义的。而在目前，多数门限签名方案不具备这种匿名性，一些方案[2–4]可以使验证者不能获知签名是由群体中哪些成员签署，但其匿名性是比较弱的，因为对于大多数带有子密钥分发中心的门限签名体制而言，分发中心一般都清楚地知道每个成员用于门限签名的子密钥是什么，故而一旦当签名的验证者与分发中心串通起来进行合谋，或者是分发中心的可信性没有保证之时，就可以判定出一个成员是否对决策进行了签名，这样表决成员的匿名性将得不到有效的保证。为此，本文基于可信平台模块TPM 1.2标准中采用的

2009-03-09 收到，2009-10-26 改回
国家自然科学基金(60503012)和国家 863 计划项目(2007AA01Z405)资助课题
通信作者: 甄鸿鹄 xtwjngn@126.com

DAA(Direct Anonymous Attestation)方案[5]，零知识证明[5,6]以及秘密共享[7,8]等技术给出一个具有强匿名性的门限签名方案，方案在签名的验证者与分发中心串通的情况下也能确保签名成员的匿名性，且签名成员每次签名之间是零关联的，因此可有效保护签名成员的隐私，其在诸如“匿名表决”等对于匿名性要求较高的场合中有着重要的应用前景。此外，本方案在确保门限签名成员强匿名性的同时，还具有子密钥不可伪造、子签名的可验证等现有门限签名方案大多不具备的特性，这些本文给出了相应的分析与证明。

2 预备知识

2.1 强 RSA 问题假设及 C-L 签名

强RSA(Rivest Shamir Adlemen)问题假设：给定一个RSA模数 $n=pq$ 和一个随机数 $c\in Z_n^*$，在不知道 n 因子分解情况下，计算 a 和 b $(a,b\in Z_n^*, b>1)$ 使得 $a^b=c \bmod n$ 的问题是困难的。

C-L(Camenisch-Lysyanskaya)签名[9]协议分为以下几个部分：

密钥生成：输入 1^k，选择大素数 p', q', p, q，其中 $p=2p'+1$，$q=2q'+1$，计算 $n=pq$，随机选择 $R_0, R_1, \cdots, R_{L-1}, S, Z\in QR_n$，输出公钥 $(n, R_0, R_1, \cdots, R_{L-1}, S, Z)$ 和私钥 p，其中 n 的长度 $\ell_n=2k$。

签名算法：对于消息 $(m_0, m_1, \cdots, m_{L-1})$，其中 $m_i\in\pm\{0,1\}^{\ell_m}$，$\ell_m$ 表示 m_i 的长度，选择一个随机素数 e，长度为 $\ell_e>\ell_m+2$，以及一个随机数 v，长度为 $\ell_v=\ell_n+\ell_m+\ell_r$，其中 ℓ_r 是安全参数。计算 A 使得 $Z\equiv R_0^{m_0}R_1^{m_1}\cdots R_{L-1}^{m_{L-1}}S^vA^e(\bmod n)$，则消息的签名是 (e, A, v)。

验证算法：为了验证 (e, A, v) 是的合法签名，检查 $Z\equiv R_0^{m_0}R_1^{m_1}\cdots R_{L-1}^{m_{L-1}}S^vA^e(\bmod n)$，并且检查 $2^{\ell_e}>e>2^{\ell_e-1}$。

C-L签名方案在强RSA假设下是安全的，证明见文献[9,10]。

2.2 DAA 方案简介

可信计算组织(Trusted Computing Group, TCG)基于可信平台模块(Trusted Platform Module, TPM)来实现平台的可信证明。但是由于TPM中的凭证密钥(Endorsement Key, EK, 其由TPM的生产厂家植入并伴随TPM寿命始终)可以唯一地标识自己，使得基于TPM来进行认证的平台用户的行为极易被人跟踪，造成隐私的泄露，因此需要实现平台的匿名认证，为此TCG在其1.2标准[11]中给出了DAA方案[5](并沿用至今)，DAA方案主要基于C-L签名及零知识证明技术构建，本质上可视为一种特殊的群签名，其安全性基础为上述的强RSA问题假设及DDH(Decisional Diffie-Hellman)问题假设[5]。

DAA方案的参与方有：可信平台模块(TPM)、主机(Host)、可信发布方(Issuer)、验证方(Verifier)，而其中TPM和Host又可统称为签名方(Signer)。其基本原理如下：Signer随机产生一个秘密数据 f (具体方案中为减少计算量将 f 拆分为 f_0 和 f_1)，并基于EK向Issuer零知识证明自己拥有 f，如果Issuer判定EK是可信的，则对 f 进行C-L签名并将签名发送给Signer，之后，Signer向Verifier零知识证明自己不仅拥有 f 而且还拥有Issuer对它的签名，如果证明通过，则Verifier相信Signer拥有可信的TPM，这样也就实现了Signer身份的匿名认证。

DAA方案发布后受到很多研究人员的关注，文献[12]对其进行了分析改进，文献[13]对其匿名性给出了度量并提出基于双线性对的实现方法，文献[14]提出了一种跨域的直接匿名认证方案，文献[15]将其应用于P2P，文献[16]应用其以实现Mobile Ubiquitous Environment中设备(如无线电话)的认证，但是将其与门限思想结合来构造匿名的门限签名算法，本文尚属首次。

2.3 基于离散对数的零知识证明的描述

为了更好地描述协议，本文将采用Camenisch和Stadler给出的标记法[17]来描述基于离散对数的零知识证明协议，例如 $\mathrm{PK}\{\alpha,\beta,\delta: y=g^\alpha h^\beta \wedge \tilde{y}=\tilde{g}^\alpha\tilde{h}^\beta \wedge (u\le\alpha\le v)\}$ 表示“关于整数 α,β,δ 的零知识证明，并且 $y=g^\alpha h^\beta$，$\tilde{y}=\tilde{g}^\alpha\tilde{h}^\beta$ 成立，同时 $(u\le\alpha\le v)$”。其中的 y, g, h, $\tilde{y}$, $\tilde{g}$, $\tilde{h}$ 是群 $G=\langle g\rangle=\langle h\rangle$ 和群 $\tilde{G}=\langle\tilde{g}\rangle=\langle\tilde{h}\rangle$ 中的元素，同时可以利用Fait-Shamir启发式[18]将零知识证明转化为对消息 m 的知识签名，可记作：$\mathrm{SPK}\{(\alpha): y=g^\alpha\}(m)$。

3 方案总体描述

3.1 方案的参与方

本方案参与方除子密钥的分发方(Dealer)，签名验证方(Verifier)，门限签名子签名成员群组(Signer<1>,Signer<2>,$\cdots$, Signer<i>,$\cdots$, Signer<n>)，还需要一个可信发布方(Issuer)。本方案中以每个 Signer 都拥有 TPM 也即都为可信计算平台的情况来讨论(且按照文献[12]的描述方法本文中不将 f 拆分为 f_0 和 f_1)，而对于没有 TPM 的情况，本方案也是适用的(这时 TPM 的操作可由主机一并完成，而 EK 可由 Signer<i>的公钥来代替)。

3.2 方案的基本思想

方案的基本思想是：任何一个签名成员

Signer<i>基于 DAA 方案通过 Issuer 向 Dealer 进行匿名认证；认证通过后，Dealer 在不知道该 Signer<i>具体是谁的情况下将一子密钥及其证书(Dealer 对该子密钥的 C-L 签名)秘密地发送给 Signer<i>；然后 Signer<i>向 Verifier 零知识证明自己拥有一个有效的子密钥并且用该子密钥计算了子签名(这样也就证明了子签名的有效性)，最后，Verifier 采用拉格朗日插值方法对于得到的有效子签名进行重构，得到最终的签名。

3.3 方案的系统结构

根据 Signer<i>交互对象的不同可将本方案划分为 3 个部分(方案系统结构如图 1 所示)，每部分及其主要任务如下。

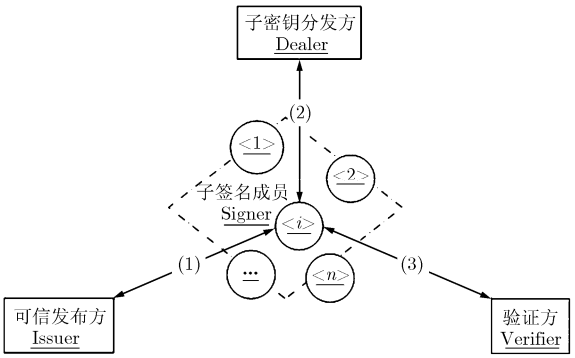

图 1 方案系统结构

(1)Signer<i>与 Issuer 的交互：Signer<i>从 Issuer 处获取 Issuer 并于自己秘密数据 f 的 C-L 签名 (e_I, A_I, v)，其中 $A_I = (Z_I/(R_I^f S_I^v))^{1/e_I} \bmod n_I$。

(2)Signer<i>与 Dealer 的交互：Signer<i>向 Dealer 证明自己所获得的 (e_I, A_I, v) 可使 $A_I \equiv (Z_I/(R_I^f S_I^v))^{1/e_I} \bmod n_I$ 成立，以实现匿名的认证，同时向 Dealer 发送一个其签名的整数 k。然后 Dealer 将已经产生好的一个门限签名子密钥 X_i 及对其的 C-L 签名秘密发送给 Signer<i>。

(3) Signer<i>与 Verifier 的交互：Signer<i>向 Verifier 零知识证明自己拥有 Dealer 发布的有效子密钥 X_i 及 Dealer 对 X_i 的 C-L 签名 (e_D, A_D, k)，并且证明子签名由 X_i 计算产生；Verifier 收集门限数量的子签名后重构门限签名。

3.4 方案的流程结构

而根据门限签名产生的过程，本方案又可划分为以下 5 个阶段：

(1)系统初始化；

(2)Dealer 生成子密钥；

(3)Signer<i>通过 Issuer 向 Dealer 进行匿名认证；

(4)Signer<i>匿名获取子密钥并产生子签名；

(5)Verifier 重构门限签名。

在对案具体协议的描述中，这 5 个阶段与第 3.3 节所述 3 个部分是相结合穿插地进行描述的，详细过程见下文。

4 具体协议流程

在对协议详细描述之前，先申明如下：本方案主要基于 DAA 方案[5]构建，而 DAA 方案又是非常复杂的，故鉴于篇幅，本文对于诸如 SPK{(α): $y = g^{\alpha}$}(m) 的零知识证明都不给出具体的过程，其详细流程请参见文献[5]，而且本文所有参数的含义及要求同文献[5]，对其也将不再进行详细的说明。

4.1 系统初始化

Issuer和Dealer都按照DAA方案所述方式生成密钥，其中Issuer的公钥为 $\mathrm{PK}_I = \{n_I, g_I', g_I, h_I, R_I, S_I, Z_I, \gamma_I, \Gamma_I, \rho_I\}$，私钥为可分解 n_I 的素数因子，基名为 bsn_I；Dealer的公钥为 $\mathrm{PK}_D = \{n_D, g_D', g_D, h_D, R_D, S_D, Z_D, \gamma_D, \Gamma_D, \rho_D\}$，私钥为可分解 n_D 的素数因子，另外还拥有一对公私钥对 $(\mathrm{PK}_D', \mathrm{SK}_D')$，基名为 bsn_D；Verifier的基名为 bsn_V。

4.2 Signer<i>通过 Issuer 向 Dealer 进行直接匿名认证

(**Signer**<i>与**Issuer**的交互)

(1)Signer<i>对Issuer的公钥进行验证(见文献[5]Appendix A)。

(2)Signer<i>秘密选择随机数 f 和 v'，计算 $U_I = R_I^f S_I^{v'} \bmod n_I$ 和 $N_I = \zeta_I^f \bmod \Gamma_I$，其中 $\zeta_I = H_I(1 \,||\, \mathrm{bsn}_I)^{(\Gamma_I - 1)/\rho_I} \bmod \Gamma_I$，$H_I(\cdot): \{0,1\}^* \to \{0,1\}^{\ell_I + \ell_\varnothing}$，并基于自己的EK将 U_I 和 N_I 发送给Issuer(见文献[5] Appendix B)。

(3)Signer<i>向Issuer零知识证明自己拥有 f 并用 f 计算了 U_I 和 N_I，也即执行如下零知识证明过程：

$$\mathrm{SPK}\{(f, v'): U_I \equiv R_I^f S_I^{v'} \bmod n_I \wedge N_I \equiv \zeta_I^f \bmod \Gamma_I \wedge f \in \{0,1\}^{\ell_f + \ell_\varnothing + \ell_H + 2} \wedge v' \in \{0,1\}^{\ell_n + \ell_\varnothing + \ell_H + 2}\}(n_s \,||\, n_i)$$

(4)Issuer检查Signer<i>的EK是否在此次门限签名的表单之中，而且对于此次门限签名而言是否第1次遇见该EK，如果都是，则选择随机数 v'' 和随机素数 e_I，$v'' \in_R [2^{\ell_v - 1}, 2^{\ell_v} - 1]$，$e_I \in_R [2^{\ell e - 1}, 2^{\ell e - 1} + 2^{\ell e' - 1}]$，计算 $A_I = (Z_I/(U_I S_I^{v''}))^{1/e_I} \bmod n_I$，将 (e_I, A_I, v'') 发送给Signer<i>，并向Signer<i>证明 (e_I, A_I, v'') 产生的正确性[5]；否则中断(这主要是阻止Signer<i>在同一次门限签名中选取不同 f 并多次运行DAA方案的Join Protocol而从Issuer处获得多个DAA证书，进而在后期从Dealer处获得多个签名

子密钥)。

(5)Signer<i>收到(e_I, A_I, v'')后计算$v = v' + v''$，则(e_I, A_I, v)将是Issuer针对Signer<i>秘密数据f的C-L签名。

(**Signer**<i>与**Dealer**的交互)

(6)Signer<i>对Dealer的公钥进行验证。

(7)Signer<i>选择随机整数$w_I, r_I \in \{0,1\}^{\ell_n+\ell_\varnothing}$，计算$T_{1I} = A_I h_I^{w_I} \bmod n_I$，$T_{2I} = g_I^{w_I} h_I^{e_I} (g'_I)^{\eta} \bmod n_I$，$\zeta_D = H_\Gamma(1 \,||\, \mathrm{bsn}_D)^{(\Gamma_I - 1)/\rho_I} \bmod \Gamma_I$，$N_D = \zeta_D^f \bmod \Gamma_I$，选取整数$k \in_R [2^{\ell_k - 1}, 2^{\ell_k} - 1]$，然后用Dealer的公钥对$k$进行加密并将加密结果$E_{\mathrm{PK}'_D}(k)$发送给Dealer，再对$E_{\mathrm{PK}'_D}(k)$进行如下零知识签名：

$$\begin{aligned}\mathrm{SPK}\{&(f, v, e_I, w_I, r_I, e_I w_I, e_I e_I, e_I r_I):\\ Z_I &\equiv \pm T_{1I}^{e_I} R_I^f S_I^v h_I^{-e_I w_I} \bmod n_I \wedge T_{2I}\\ &\equiv \pm g_I^{w_I} h_I^{e_I} (g')_I^{\eta_I} \bmod n_I \wedge 1\\ &\equiv \pm T_{2I}^{-e_I} g_I^{e_I w_I} h_I^{e_I e_I} (g')_I^{e_I r_I} \bmod n_I \wedge N_D\\ &\equiv \zeta_D^f \bmod \Gamma_I \wedge f \in \{0,1\}^{\ell_f + \ell_\varnothing + \ell_H + 2} \wedge\\ &(e - 2^{\ell_e}) \in \{0,1\}^{\ell'_e + \ell_\varnothing + \ell_H + 1}\}(n_s \,||\, n_d \,||\, E_{\mathrm{PK}'_D}(k))\end{aligned}$$

并输出签名$\sigma_I = (\zeta_D, (T_{1I}, T_{2I}), N_D, c, n_s, (s_v, s_f, s_{e_I}, s_{e_I e_I}, s_{w_I}, s_{e_I w_I}, s_{r_I}, s_{e_I r_I}))$。

(8)Dealer对零知识签名σ_I进行验证(见文献[5])，验证通过则Signer<i>实现了向Dealer的匿名认证，同时Dealer解密$E_{\mathrm{PK}'_D}(k)$获得数据k，$k = D_{\mathrm{SK}'_D}(E_{\mathrm{PK}'_D}(k))$。自此，虽然Dealer并不知道与“假名”$N_D$(因为$N_D$可作为一个标识Signer<$i$>的代号)相对应着的Signer<$i$>是谁，但Dealer相信该Signer<$i$>具有进行门限签名的资格，须将一个子密钥发送给他，这便进入了下一阶段。

4.3 Dealer 生成签名子密钥

Dealer基于Feldman可验证秘密共享方案[8]产生用于(n,t)门限签名的子密钥：

(1)对于秘密信息$X \in Z_q^*$随机选择$t-1$个Z_q^*中的元素$a_1, a_2, \cdots, a_j, \cdots, a_{t-1}$，定义$Z_q^*[x]$中一个$t-1$次多项式：$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$，其中$a_0 = X$；

(2)计算$X_1, X_2, \cdots, X_i, \cdots, X_n$作为子密钥，其中$X_i = F(i) \bmod \rho_D$；

(3)公布或广播$Y_0, Y_1, Y_2, \cdots, Y_j, \cdots, Y_{t-1}$，其中$Y_j = \gamma_D^{a_j} \bmod \Gamma_D$。

值得说明的是：Feldman方案至今仍被认为是性能优秀的且被大量引用的可验证秘密共享方案；Dealer的公钥中参数$\gamma_D, \Gamma_D, \rho_D$[5]正好满足Feldman方案[8]对参数的要求(Γ_D为大素数，ρ_D是$\Gamma_D - 1$的素因子，γ_D是$Z_{\Gamma_D}^*$中一个ρ_D阶元素)；且基于Feldman秘密共享方案本文作者还提出了一种容忍入侵的会议密钥分配方案[19]。

4.4 Signer<i>匿名获取子密钥并产生子签名

在Signer<i>通过Dealer匿名认证，且Dealer已经产生好子签名密钥X_i之后，便进入本过程阶段：

(1)为防止同一个Signer<i>冒领多个子密钥，Dealer检查Signer<i>在第4.2节中发送来的N_D是否已经遇见过，若是则中断后续操作，如果没有，则继续后续操作。

(2)对于任一子密钥X_i(其生成见本文第4.3节)，Dealer选择素数$e_D \in_R [2^{\ell_e - 1}, 2^{\ell_e - 1} + 2^{\ell_{e'} - 1}]$，计算$A_D = (Z_D / (R_D^{X_i} S_D^k))^{1/e_D} \bmod n_D$，并秘密发送$(e_D, A_D, X_i)$给Signer<$i$>，同时向Signer<$i$>零知识证明$A_D$计算的正确性：$\mathrm{SPK}\{(d_D): A_D \equiv (Z_D / (R_D^{X_i} S_D^k))^{d_D} \bmod n_D\}(n_s)$。而Signer<$i$>得到$(e_D, A_D, X_i)$，意味着其不仅得到了一个签名子密钥$X_i$，同时根据C-L签名的定义其也得到了Dealer对X_i的C-L签名(e_D, A_D, k)。

(3) Signer<i>验证子密钥X_i的有效性：检验是否$\gamma_D^{X_i} \equiv \prod_{j=0}^{t-1} Y_j^{i^j} \bmod \Gamma_D$，如果成立，$X_i$就是有效的，否则$X_i$不是由Dealer产生的子密钥，Signer<$i$>可进行检举。

(**Signer**<i>与**Verifier**的交互)

(4)Signer<i>选择随机整数$w_D, r_D \in \{0,1\}^{\ell_n + \ell_\varnothing}$，计算$T_{1D} = A_D h_D^{w_D} \bmod n_D$，$T_{2D} = g_D^{w_D} h_D^{e_D} (g')_D^{r_D} \bmod n_D$，以及$H_{mV} = H_\Gamma(m \,||\, \mathrm{bsn}_V)^{(\Gamma_D - 1)/\rho_D} \bmod \Gamma_D$，$\mathrm{Sign}_{imV} = H_{mV}^{X_i} \bmod \Gamma_D$，其中$m$为需要门限签名(也即需要匿名表决)的数据或消息，$H_{mV}$为$m$的特定摘要，$\mathrm{Sign}_{imV}$为Signer<$i$>针对$m$的子签名。

(5)Signer<i>向Verifier零知识证明，自己不仅拥有Dealer颁发的签名子密钥X_i及其证书(Dealer对X_i的C-L签名)，同时还用X_i计算了子签名Sign_{imV}：

$$\begin{aligned}\mathrm{SPK}\{&(X_i, k, e_D, w_D, r_D, e_D w_D, e_D e_D, e_D r_D):\\ Z_D &\equiv \pm T_{1D}^{e_D} R_D^{X_i} S_D^k h_D^{-e_D w_D} \bmod n_D \wedge T_{2D}\\ &\equiv \pm g_D^{w_D} h_D^{e_D} (g')_D^{r_D} \bmod n_D \wedge 1\\ &\equiv \pm T_{2D}^{-e_D} g_D^{e_D w_D} h_D^{e_D e_D} (g')_D^{e_D r_D} \bmod n_D \wedge \mathrm{Sign}_{imV}\\ &\equiv H_{mV}^{X_i} \bmod \Gamma_D \wedge X_i \in \{0,1\}^{\ell_{X_i} + \ell_\varnothing + \ell_H + 2}\\ &\wedge (e_D - 2^{\ell_e}) \in \{0,1\}^{\ell'_e + \ell_\varnothing + \ell_H + 1}\}(n_s \,||\, n_v)\end{aligned}$$

(6)上述零知识证明通过Verifier的验证后(同DAA方案的Verification Algorithm[5])，子签名过程结束，同时也证明了子签名Sign_{imV}的有效性(也即正确性)。

4.5 Verifier 重构门限签名

当 t 个子签名 $\mathrm{Sign}_{i_1mV},\mathrm{Sign}_{i_2mV},\cdots,\mathrm{Sign}_{i_tmV}$ 通过验证之后，Verifier可根据格朗日插值计算 $\mathrm{Sign}_{mV}=\prod_{s=1}^{t}=\mathrm{Sign}_{i_smV}^{b_{i_s}} \bmod \Gamma_D = H_{mV}^{X}$，其中 $b_{i_s}=\prod_{j=1,j\neq s}^{t}\frac{i_j}{i_s-i_j} \bmod \rho_D$，尽而重构出对于数据 m 的整体门限签名。由于所有的子签名的正确性都是经过验证的，故 Sign_{mV} 必定是有效的门限签名结果(Verifier无需对其进行其它的验证)。而就 (n,t) 匿名表决而言，只要有 t 个子签名通过验证，则表明有关决议或数据 m 的表决已经获得了通过。

5 分析与证明

5.1 方案性能分析

本方案可用于解决匿名表决等一些实际问题，且根据表决人员 n、表决门槛 t 及表决内容 m 的不同情况，下一次匿名表决无须从头开始，可从上次表决过程中间开始，这样可节省一部分的时间开销，具体讨论如下：

$(n,t,\overline{m})$ 表示本次表决与上次表决的人员与门槛相同，而表决内容不同，对于这种情况表决可以直接从第3.3节所述第(3)部分“Signer<i>与Verifier的交互”开始，反映在具体协议流程中，可直接从第4.4节第(4)小节处开始；

$(n,\overline{t},\overline{m})$ 表示本次表决与上次表决的人员相同，而表决的门槛及内容不同，对于这种情况表决可以直接从第3.3节所述第(2)部分“Signer<i>与Dealer的交互”开始，反映在具体协议流程中，可直接从第4.2节第(6)小节处开始；

$(\overline{n},\overline{t},\overline{m})$ 表示本次表决与上次表决的人员、门槛、内容都不同，对于这种情况需要从第3.3节所述第(1)部分“Signer<i>与Issuer的交互”开始，反映在具体协议流程中，可从第4.2节第(1)小节处开始。

5.2 方案特性分析

本方案具有如下特性：

(1)子密钥的可验证性：Signer<i>可判断 X_i 是否由Dealer产生。

证明　略，此特性是本文所采用的Feldman可验证秘密共享方案的特性[8]。

(2)子密钥的不可伪造性：Signer<i>都不可能伪造子密钥 X_i。

证明　本方案中子密钥 X_i 有效意味着 X_i 拥有相应的证书，也即拥有Dealer对于 X_i 的C-L签名。Signer<i>可伪造子密钥 X_i 进行签名，意味着其可计算 $A_D=(Z_D/(R_D^{X_i}S_D^k))^{1/e_D} \bmod n_D$，但这与强RSA问题假设相矛盾，因为其不可能对大数 n_D 进行因子分解。

(3)子签名的可验证性：只要本文第4.4节第(5)小节所述零知识证明获得通过，则相应 $Sign_{iV}$ 就是有效的。

证明　Signer<i>只有拥有Dealer颁发的 X_i 及关于 X_i 的证书 (e_D,A_D,k)，上述零知识证明才能通过。反之，上述零知识证明获得通过，则表明Signer<i>拥有 X_i 的证书 (e_D,A_D,k) 且用该 X_i 计算了子签名 Sign_{iV}。因此，只要通过了验证，Signer<i>就是用有效的子密钥 X_i 计算了子签名 Sign_{iV}，而 Sign_{iV} 就是有效的子签名。

(4)子签名的零关联性：在 $(n,t,\overline{m})$ 的情况下，Verifier不能判定两个子签名 $\mathrm{Sign}_{im_1V}=(H_\Gamma(m_1\,||\,\mathrm{bsn}_V)^{(\Gamma_D-1)/\rho_D} \bmod \Gamma_D)^{X_i}$ 和 $\mathrm{Sign}_{im_2V}=(H_\Gamma(m_2\,||\,\mathrm{bsn}_V)^{(\Gamma_D-1)/\rho_D} \bmod \Gamma_D)^{X_i}$ 是否由同一个签名者Signer<i>使用相同的子密钥 X_i 签署。

证明　由于Verifier始终不知道 X_i，因此Verifier只有在可求解 X_i 的情况下才可做出 Sign_{im_1V} 与 Sign_{im_2V} 是否关联的判断，但是求解 X_i 是个离散对数问题。

(5)方案的强匿名性：在 $\mathrm{bsn}_I\neq\mathrm{bsn}_D$ 的情况下，即使Verifier、Dealer彼此串通，Signer<i>的匿名性能够始终保持。

证明　在 $\mathrm{bsn}_I\neq\mathrm{bsn}_D$ 的情况下，$N_D\neq N_I$，Dealer与Issuer之间将没有可供关联的数据，也就没有串通的依据或串通Issuer将不起任何作用，所以只能是Verifier、Dealer进行串通。但是，(a)Verifier无法知道子签名 Sign_{iV} 对应着的签名人是谁，因为子签名是通过零知识证明得到的；(b)Dealer无法知道Signer<i>具体是谁，尽管Dealer将子密钥 X_i 发给了Signer<i>，之所以Dealer相信Signer<i>是签名成员中的一员，是因为Signer<i>利于DAA方案向Dealer进行了匿名认证，而DAA方案的功能就是在于能够实现认证者的匿名；(c)既然Verifier和Dealer都无法知道子签名 Sign_{iV} 对应着的签名人是谁，串通将没有意义。

基于以上，Signer<i>的匿名性能够始终保持，这种强匿名性使得签名具有不可追踪性，且Verifier和Dealer在实际应用中也可以是同一个实体。而对于 $\mathrm{bsn}_I=\mathrm{bsn}_D$ 这种特殊情况(其相当于Issuer和Dealer为同一个实体)，方案中Verifier, Dealer, Issuer若进行3方合作(或串通)便可获知 Sign_{iV} 对应着的签名人是谁(该过程的追踪链为 $\mathrm{Sign}_{imV}\rightarrow X_i\rightarrow N_D=N_I\rightarrow EK\rightarrow$ Signer<i>，其原理同文献[20]第4.2节中对DAA方案匿名性的讨论)，因此方案

的匿名性将变弱，而方案本身也退化成为一个可追踪的门限签名方案，故对于匿名性有较高要求的情况下，应当确保方案的强匿名性，也即必须满足 $\mathrm{bsn}_I \neq \mathrm{bsn}_D$。

(6)方案的鲁棒性：当恶意攻击者控制的签名成员人数少于 t 时，其不能伪造签名。

证明 Verifier 在对 t 个子签名 $\mathrm{Sign}_{i_1 mV}$, $\mathrm{Sign}_{i_2 mV},\cdots,\mathrm{Sign}_{i_t mV}$ 的有效性进行验证之后，才可重构签名，且由于重构采用的Feldman方案是 (n,t) 门限的，故当恶意攻击者控制的签名成员(强迫其进行子签名有效性的证明，也即强迫其进行匿名表决)人数少于 t 时，其不能伪造整体的门限签名。

(7)方案的正确性：如果DAA方案和Feldman门限方案是安全的，那么方案在可确保子签名成员强匿名性的同时，必能得到正确的签名结果。

证明 本方案在本质上是对DAA方案的拓展性应用。方案的证明完全可以按照DAA方案的证明方式(文献[5]完整版之Appendix C)进行，鉴于篇幅，不再详述。而其中所用Feldman门限方案的安全性见文献[8]。在本方案中子签名具有不可伪造性(否则DAA方案就是可伪造的)，而在子签名不可伪造的情况下，最终的门限签名必定是正确的，其作为“表决”结果必然是有效的。

6 结束语

本文提出了一种基于DAA的强匿名性门限签名方案，方案的强匿名性，可使签名成员的身份隐私得到强有力保护，这使得方案在“匿名表决”等对匿名性有较高要求的场合下有着重要的应用价值。除具有强匿名性外，本方案还具有子签名可验证等特性。方案不仅在可信计算平台环境下易于构建，对于没有TPM的情况也是实用的(子签名可全部由主机实现)，因此也具有较强的适用性。

参 考 文 献

[1] Desmedt Y and Frankel Y. Shared generation of authenticators and signatures[C]. Advances in Cryptology-Crypto'91 Proceedings Ee1, Berlin, 1992, Vol. 576: 457–469.

[2] Wang Gui-lin, Han Xiao-xi, and Zhu Bo. On the security of two threshold signature schemes with traceable signers[C]. ACNS 2003, Kunming China, 2003, Vol.2846: 111–122.

[3] 刘锋, 张建中. 基于 Williams 体制的门限签名方案[J]. 计算机应用研究, 2006, 23(6): 108–109.
Liu Feng and Zhang Jian-zhong. Threshold group signature scheme based on Williams scheme[J]. *Application Research of Computers*, 2006, 23(6): 108–109.

[4] Zheng Dong, Li Xiang-xue, and Ma Chang-she, *et al*.. Democratic group signatures with threshold traceability. http://eprint.iacr.org/2008/112, 2008. (Cryptology ePrint Archive: Report 2008/112).

[5] Brickell E, Camenisch J, and Chen Li-qun. Direct anonymous attestation[C]. Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington DC(US), 2004: 132–145.(A full version of this paper available at http://eprint.iacr.org/2004/205/).

[6] Brickell E. An efficient protocol for anonymously providing assurance of the container of a private key[R]. Submitted to the Trusted Computing Group, 2003.

[7] Shamir A. How to share a secret[J]. *Communications of ACM*, l979, 22(11): 6l2–6l3.

[8] Feldman P and Practical A. Scheme for non-interactive verifiable secret sharing[C]. Proc of 28th Annual Symposium, New York, 1987: 427–437.

[9] Camenisch J and Lysyanskaya A. A signature scheme with efficient protocols[C]. Security in Communication: Third International Conference, Italy, 2003, Vol.2576: 268–289.

[10] Camenisch J and Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials[C]. Advances in Cryptology-CRYPTO 2002, Santa Barbara, California, USA, 2002, Vol.2442: 61–76.

[11] Trusted Computing Group. TCG TPM specification 1.2[OL/EB]. 2003, Available at http://www.trusted computinggroup. org.

[12] Brickell E and Li Jiang-tao. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities[C]. The 6th Workshop on Privacy in the Electronic Society (WPES), Alexandria, Virginia, 2007: 21–30.

[13] Brickell E, Chen Li-qun, and Li Jiang-tao. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings[C]. The Conference on Trusted Computing (TRUST 2008), Villach, Austria, 2008: 315–330.

[14] 陈小峰, 冯登国. 一种多信任域内的直接匿名证明方案[J]. 计算机学报, 2008, 31(7): 1122–1130.
Chen Xiao-feng and Feng Deng-guo. A direct anonymous attestation scheme in multi-domain environment[J]. *Chinese Journal of Computers*, 2008, 31(7): 1122–1130.

[15] Balfe S, Lakhani A D, and Paterson K G. Securing peer-to-peer networks using trusted computing[C]. Chapter 10 of Trusted Computing, London, 2005: 271–298.

[16] Leung A and Mitchell C J. Ninja: Non identity based, privacy preserving authentication for ubiquitous environments[C]. Proceedings of 9th International Conference on Ubiquitous Computing, Innsbruck, Austria, 2007, Vol.4717: 73–90.

[17] Camenisch J and Stadler M. Efficient group signature schemes for large groups[C]. Advances in

Cryptology-CRYPTO'97, Santa Barbara, California, USA, 1997, Vol.1296: 410–424.

[18] Fiat A and Shamir A. How to prove yourself: Practical solutions to identification and signature problems[C]. Advances in Cryptology-CRYPTO'86, Santa Barbara, California, USA, 1987, Vol.263: 186–194.

[19] 郭渊博, 马建峰. 一种容忍入侵的会议密钥分配方案[J]. 西安电子科技大学学报(自然科学版), 2004, 31(2): 260–263.
Guo Yuan-bo and Ma Jian-feng. An intrusion-tolerant conference key distribution scheme[J]. *Journal of Xidian University*, 2004, 31(2): 260–263.

[20] Smyth B, Ryan M, and Chen Li-qun. Direct Anonymous Attestation (DAA): Ensuring privacy with corrupt administrators[C]. Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks, Lecture Notes in Computer Science (LNCS), Cambridge, UK, 2007, Vol.4572: 218–231.

甄鸿鹄：　男，1983 年生，硕士，工程师，研究方向为可信计算、网络信息安全.

陈　越：　男，1965 年生，博士，教授，博士生导师，研究方向为网络安全、对等通信.

郭渊博：　男，1975 年生，博士，副教授，硕士生导师，研究方向为分布式容忍入侵、网络信息安全.