一种高效的(t,n)门限群签名方案

刘丹妮[1,2] 王兴伟[1] 郭 磊[1] 黄 敏[1]
(东北大学信息科学与工程学院 沈阳 110004)[1] (大连东软信息学院计算机科学与技术系 大连 116023)[2]

摘 要 基于离散对数和秘密共享思想,提出一个高效的(t,n)门限群签名方案。份额分配中心DC(Distribution Center)以自选份额的形式与群中成员共享签名密钥。SC(Signature Combiner)对收到的份额签名进行身份验证和签名正确性验证,然后合成签名。份额签名成员的身份和合成签名的时间戳被记录在数据库中,以备仲裁者将来打开签名使用。最后从正确性、安全性和效率三方面进行了分析,结果表明本方案是一个高效安全的门限群签名方案。

关键词 门限群签名,秘密共享,数字签名
中图法分类号 TP393 **文献标识码** A

Efficient Scheme of (t,n) Threshold Group Signature

LIU Dan-ni[1,2] WANG Xing-wei[1] GUO Lei[1] HUANG Min[1]
(School of Information Science & Engineering, Northeastern University, Shenyang 110004, China)[1]
(Department of Computer Science & Technology, Dalian Neusoft Institute of Information, Dalian 116023, China)[2]

Abstract An efficient threshold signature scheme based on the difficulty of discrete logarithm problem and secret sharing method was proposed. Distribution Center(DC) shares the signature secret key with group members by the method of optional quotient. DC generates threshold Signature according to the sharing signatures after the identity and correctness verification. The identity and time stamp of the sharing signature members are recorded in the database prepared for arbitrating the dispute in the future. The analysis from correctness, security and efficiency shows that the proposed scheme is effective and secure.

Keywords Threshold group signature, Secret sharing, Digital signature

数字签名在当今的电子商务系统中起着重要作用。很多场合下,需要多人同时参与,签名才能生效,这需要将签名密钥分给多人掌管,并同时参与才能生成合法的签名,即是群签名的思想。门限签名方案允许群中 t 个或更多参与者代表群联合产生有效签名。签名过程中成员生成份额签名没有先后顺序,必须由一个签名收集者最终合成整个签名。与普通的群签名方案相比,门限签名具有更高的安全性,成为数字签名的重要分支。第一个门限签名方案是基于RSA密码体制和Shamir的秘密共享思想,由Desmedt和Frankel于1991年提出[1]。之后,门限签名得到广泛研究,提出了各种各样的门限群签名方案。根据密钥的分发方式的不同,现有的门限群签名方案可以分为两种类型:带有秘密分发中心的门限群签名方案[2-4]和分布式分发分存秘密的门限群签名方案[5-10]。Wang等人于2000年提出的群签名方案[7]将群成员分成(t,n)门限签名组和(k,l)门限验证组,由 t 个签名组参与者生成联合签名,由 k 个验证组成员共同验证签名的合法性,所有成员签名和验证的密钥由分发中心SDC分发,是群签名研究的一个重要进展。随后,Hsu等人[8]指出该方案在每次签名时总是使用相同的会话密钥,所以攻击者可以通过两个有效门限签名破译群密钥,然后进行伪造签名。为此Hsu等人对该方案进行了改进,使得每次签名的会话密钥都不同,从而提高了完全性。但是改进后的方案签名组成员生成签名的参数需要1024位,计算效率很低,而且签名组与验证组的成员不能互相变换角色。

文中基于文献[11]的秘密共享思想,采用基于离散对数的DSA变形,提出一种新的比文献[7,8]更高效的门限群签名方案,所有成员既可以参与签名,也可以作为验证者接收签名;份额密钥泄露不会导致签名方案受到攻击。分析表明,该方案具有签名不可伪造性、不诚实签名可识别性、身份可追查性等安全特性,因为在份额签名和合成签名中使用的都是160位,而且所有签名成员将份额签名都发送给SC,无需发送给所有其他成员,所以在运算效率和网络传输量方面具有优势,是一个高效的门限群签名方案。

1 提出的门限群签名方案

本方案中包括3个实体:份额分配中心DC(Distribution

到稿日期:2010-02-09 返修日期:2010-04-28 本文受国家自然科学基金项目(60673159,70671020,70931001,60802023),国家高技术研究发展计划项目(2007AA041201),国家科技支撑计划项目(2008BAH37B03,2008BAH37B07),高等学校博士学科点专项科研基金资助课题(20070145017),中央高校基本科研业务费(N090504003,N090504006)资助。
刘丹妮(1975—),女,博士生,主要研究方向为信息安全,E-mail:liudanni@neusoft.edu.cn;王兴伟(1968—),男,教授,博士生导师,主要研究方向为网络安全。

Center)、群成员、签名合成者 SC(Signature Combiner)。SC 对接收的份额签名进行身份验证和正确性验证,只有合法签名才能合并到联合签名中。最终签名需要 SC 协助产生,同时 SC 也要产生一个份额签名,以增加安全性。

1.1 系统建立

系统生成公共参数,秘密选取大素数 p ,q 和公开的 Hash 函数 $H(.)$,满足 $q|p-1$,$2^{511}<p<2^{1024}$,$2^{159}<q<2^{160}$,而且在 Z_p^* 中求解离散对数是困难的;$g\in Z_p^*$,且满足 $g=h^{(p-1)/q} \bmod p$,其中 h 是 $1<h<p-1$ 的整数,$h^{(p-1)/q} \bmod p>1$。p,q,g 是系统参数,在系统内公开。其中 p 大于 512 位,它满足 Z_p 中的离散对数问题是难解决的。

1.2 份额密钥生成

份额分配中心 DC 为群成员分配份额密钥。有群成员 $P_1,P_2,\cdots,P_n$ 中,只有至少 t 个成员对消息 m 签名后,才能生成合法签名。对于 n 个成员,最多有 C_n^t 种组合,所有组合可表示成[10]:

第 1 组:$Q_{11},Q_{12},\cdots,Q_{1t}$

第 2 组:$Q_{21},Q_{22},\cdots,Q_{2t}$

$\vdots$

第 C_n^t 组:$Q_{C_n^t 1},Q_{C_n^t 2},\cdots,Q_{C_n^t t}$

简写为:Q_{ji},$j=1,2,\cdots,C_n^t$,$i=1,2,\cdots,t$。j 表示各个分组的组号,i 表示组中成员的序号。$Q_{ji}\in\{P_1,P_2,\cdots,P_n\}$。

每个成员 P_i 选择随机数 $x_{P_i}\in Z_p^*$,$i=1,2,\cdots,n$ 作为 P_i 的私钥,计算 $y_i=g^{x_{P_i}} \bmod p$,将公钥 y_i 公开。将 x_{P_i} 通过安全信道发送给 DC,选择随机数 $x_{DC}\in Z_p^*$,要求 $x_{DC}>\sum_{i=1}^{n}x_{P_i}$,计算 SC 协助第 j 组签名的秘密份额 D_j:

$$D_j=x_{DC}-\left(\sum_{i=1}^{t}x_{Q_{ji}}\right),j=1,2,\cdots,C_n^t$$

$$Q_{ji}\in\{P_1,P_2,\cdots,P_n\}$$

式中,$x_{Q_{ji}}$ 是成员 Q_{ji} 的私钥。于是生成 SC 协助签名份额密钥与各门限小组的关系对:

$$\langle D_j,(Q_{j1},Q_{j2},\cdots,Q_{jt})\rangle \tag{1}$$

式中,j 是组号,$Q_{j1},Q_{j2},\cdots,Q_{jt}\in\{P_1,P_2,\cdots,P_n\}$,表示 $Q_{j1},Q_{j2},\cdots,Q_{jt}$ 构成 (t,n) 门限签名第 j 小组。DC 将式(1)的关系对保存下来,同时丢弃 x_{P_i},$(i=1,2,\cdots,n)$ 和 x_{DC}。DC 将 D_j 发给 SC,以备将来 SC 通过 D_j 作为签名子密钥协助第 j 组完成签名。

1.3 发出签名申请

成员 P_i 向 DC 发出对消息 m 的签名申请,DC 选择一组成员 $\langle Q_{j1},Q_{j2},\cdots,Q_{jt}\rangle$,$j\in\{1,2,\cdots,C_n^t\}$,进行联合签名。

为后文叙述方便,简称该组成员为 $\langle Q_1,Q_2,\cdots,Q_t\rangle$,令该组成员签名份额密钥为 $(x_1,x_2,\cdots,x_t)$,SC 协助签名的密钥份额 D_j 记为 x_0。$y_0=g^{x_0} \bmod p$,将公钥 y_0 公开。

DC 将 $P_i,m,\langle Q_1,Q_2,\cdots,Q_t\rangle$ 和时间戳记录在数据库中,以备将来发生纠纷时,打开签名使用。

1.4 生成份额签名

DC 将待签消息 m 以组播方式发给成员 $\langle Q_1,Q_2,\cdots,Q_t\rangle$,将 m 和参与签名的成员列表发给 SC,以备 SC 合成签名时使用。成员 $Q_i(i=1,2,\cdots,n)$ 选取随机数 $k_i,d_i\in Z_p^*$,计算:

$$\begin{aligned}&r_i=g^{k_i} \bmod q,v_i=k_i d_i \bmod q\\&s_i=(H(m)+x_i r_i)d_i \bmod q\\&u_i=x_i r_i^2 \bmod q\end{aligned} \tag{2}$$

Q_i 将 (r_i,v_i,s_i,u_i) 作为份额签名发给签名合成者 SC。

1.5 合成签名

SC 首先验证 (r_i,v_i,s_i,u_i) 确实由成员 Q_i 生成,计算:

$$\begin{aligned}&r_i'=(g^{H(m)w_i(\bmod p)}y_i^{r_i w_i(\bmod p)})\bmod p \bmod q\\&w_i=(v_i/s_i) \bmod q\end{aligned} \tag{3}$$

若 $r_i'=r_i$,则确认签名 (r_i,v_i,s_i,u_i) 由 Q_i 发出。

SC 用 x_0 作为子密钥协助签名,生成 SC 的份额签名 (r_0,v_0,s_0,u_0),选取随机数 $k_0,d_0\in Z_p^*$,计算:

$$r_0=g^{k_0} \bmod q,v_0=k_0 d_0 \bmod q$$

$$s_0=(H(m)+x_0 r_0)d_0 \bmod q,u_0=x_0 r_0^2 \bmod q$$

SC 将所有份额签名合并:

$$S=\prod_{i=0}^{t}r_i^{s_i} \bmod q,R=\sum_{i=0}^{t}r_i \bmod q,R=\sum_{i=0}^{t}r_i \bmod q \tag{4}$$

SC 将合成签名 (S,R,δ) 发送给发起者 P_i。将 (S,R,δ)、消息 m、参与签名的群成员列表和生成合成签名的时间戳作为一条记录存在 SC 的数据库中,以备将来追查签名人。

SC 按照式(2)生成身份签名 (r_{SC},v_{SC},s_{SC}),将其与 (S,R,δ)、消息 m 一同发送给接收者 B。

1.6 验证签名

B 收到签名和消息 m 后,应用式(3)判断,若 $r_0'=r_0$,则验证签名确实由 SC 发出,然后计算:

$$S'=\prod_{i=0}^{t}g^{(H(m)R+\delta)\bmod q} \bmod p \bmod q$$

若 $S'=S$ 成立,则签名验证通过,确认签名通过 SC 由 t 个合法成员联合生成。

2 正确性分析

定理 1 群成员个体使用式(2)签名,接收者应用式(3)计算 r_i',当 $r_i'=r_i$ 条件成立时,接收者确认签名由该成员发出。

证明:接收者计算 r_i':$w_i=(v_i/s_i) \bmod q$

$$r_i'=(g^{H(m)w_i(\bmod q_i)}y_i^{r_i w_i(\bmod q_i)}) \bmod p \bmod q=r_i$$

$$\begin{aligned}r_i'&=(g^{H(m)w_i(\bmod q_i)}y_i^{r_i w_i(\bmod q_i)}) \bmod p \bmod q\\&=(g^{(H(m)w_i+x_i r_i w_i)(\bmod q_i)}) \bmod p \bmod q\\&=(g^{w_i(H(m)+x_i r_i)(\bmod q_i)}) \bmod p \bmod q\\&=(g^{v_i(H(m)+x_i r_i)/s_i(\bmod q_i)})\bmod p \bmod q\\&=(g^{k_i(\bmod q_i)}) \bmod p \bmod q\\&=(g^{k_i})\bmod p \bmod q\\&=r_i\end{aligned}$$

所以定理得证。

定理 2 按照式(4)将份额签名合并,使其最终能通过接收者的验证。

证明:$r_i^{s_i}=(g^{k_i d_i(H(m)+x_i r_i)\bmod q} \bmod p) \bmod q$

$$\begin{aligned}&=(g^{v_i(H(m)+x_i r_i)\bmod q} \bmod p) \bmod q\\&=(g^{v_i H(m)\bmod q}\cdot g^{x_i r_i \bmod q}) \bmod p \bmod q\end{aligned}$$

$$\begin{aligned}S&=\prod_{i=0}^{t}r_i^{s_i} \bmod p \bmod q\\&=g^{\left(\sum_{i=0}^{t}v_i H(m)\right)\bmod q}\cdot g^{\sum_{i=0}^{t}x_i r_i \bmod q} \bmod p \bmod q\\&=g^{\left(\sum_{i=0}^{t}v_i H(m)\right)\bmod q}\cdot g^{\sum_{i=0}^{t}u_i \bmod q} \bmod p \bmod q\end{aligned}$$

因为 $R=\sum_{i=0}^{t}r_i \bmod q,\delta=\sum_{i=0}^{t}u_i \bmod q$

所以 $S=\prod_{i=0}^{t}g^{(H(m)R+\delta)\bmod q} \bmod p \bmod q=S'$。证毕。

3 安全性分析

定理 3 该门限签名方案生成的份额签名和合成签名都具有不可伪造性。

证明：

(1)在份额签名阶段生成的签名，发送给签名合成者 SC，SC 对收到的签名首先进行身份验证。只有合法成员的签名才能被接受。对签名者身份的验证可根据定理 1，当 $r_i'=r_i$ 成立时，表明签名确实由合法成员 Q_i 发出，则接受签名。

(2)合成签名接收者 B 收到 SC 的合成签名后，使用 SC 的公钥应用式(3)验证 $r_0'=r_0$ 是否成立，如果成立，则合成签名是由 SC 参与、同 t 个成员共同生成。

定理 4 该门限签名方案对不诚实签名者进行的签名具有可识别性。

证明：(1)反证法。份额签名生成阶段，假设有非法成员 J 冒充 Q_i 进行不诚实签名，SC 经过验证却未识别出该签名，即 $r_j'=r_j$，得出 J 的公钥 y_j 与 Q_i 的 y_i 相等，因为 $y_i=g^{x_i} \bmod p$，所以 J 冒充 I，前提需要根据 I 的公钥解出 x_i，即 J 解决了离散对数问题，与离散对数问题难解相悖，所以份额签名生成阶段 J 的不诚实签名能够被 SC 识别。

(2)同理，合成签名接收者收到 SC 的合成签名后，如果有人冒充 SC 生成合成签名，也会被 SC 识别。

定理 5 合法群成员参与签名后，对其签名具有不可否认性，其身份具有可追查性。

证明：(1)签名发起者 P_i 向 DC 发出签名申请，DC 验证其身份合法后，会将 P_i 记录在数据库中，便于以后发生纠纷时追查。所以 P_i 不可否认发出此次签名申请的事实，将来 DC 能追查出其身份。

(2)份额签名发送给 SC 后，SC 验证签名者身份。当所有签名成员的身份验证通过后，SC 合成签名，并在数据库中记录下此次合成签名信息、参与此次签名的所有成员和时间戳。当成员间发生签名纠纷时，SC 找到相应记录，追查出所有签名成员，并且签名成员不可否认对其的责任。

(3)合成签名必须有 SC 生成的份额签名与其他成员合作才能得到合成签名。SC 只有认同份额签名者的合法身份和份额签名的有效性，才会参与签名。

综上，合法成员参与签名后，不可否认自己生成了份额签名，SC 能追查出其身份。证毕。

4 效率分析与比较

在份额签名生成阶段，文献[8]中需要私有参数 2 个($(f_s(x_{si}), f_b(x_{si}))$)，公有参数 3 个($y_{si}, y_{vj}, y_h$)，而本方案私有参数($x_i$)和公有参数($y_i$)各 1 个。份额签名生成后，需要由签名成员将其传送给签名合成者。文献[8]中每个签名成员需要将 r_{si} 发送给 S 中其他所有成员，利用收集到的所有 r_{si} 生成自己的签名 s_i 发送给 CLK。因为 r_{si} 是 1024 位，s_i 是 160 位，所有网络传输量为 $(t-1)*1024*t+t*160$ 位。本方案中所有签名成员将签名(r_i, v_i, s_i, u_i)发送给 SC。r_i, v_i, s_i, u_i 都是 160 位参数，所以份额签名传送时共产生 $t*4*160$ 位的网络传输量，显然明显少于文献[8]的传输量。

文献[8]中份额签名产生和验证阶段 r_{s_i} 中涉及模幂、模乘和逆运算，其时间复杂度达到 $O((\log n)^3)$。在本方案的份额签名产生阶段，r_i, v_i, u_i 都可以采用预处理的方式，在签名之前，成员可以预先选取随机数 k_i 和 d_i，计算出 r_i, v_i, u_i，待消息 m 产生后，再计算 s_i。份额签名和验证阶段的时间复杂度主要取决于 s_i 的计算过程，其时间复杂度为 $O((\log n)^2)$，效率上优于文献[8]。同样，在群签名的产生和验证阶段，文献[7]的时间复杂度为 $O((\log n)^3)$，本文为 $O((\log n)^2)$。

文献[8]中的群成员不能同时为签名者和验证者。只能有一种身份。而本文中的成员可以同时具备两种身份。

关于效率的分析，如表 1 所列。

表 1 本文方案与文献[8]的效率比较

方案	份额签名参数		网络传输信息量	份额签名时间复杂度	群签名时间复杂度
	私有	公开			
Hsu	2	3	$(t-1)*1024*t+t*160$	$O((\log n)^3)$	$O((\log n)^3)$
本文	1	1	$t*4*160$	$O((\log n)^2)$	$O((\log^n)^2)$

结束语 本文基于秘密共享思想，采用基于离散对数的 DSA 变形，提出一种新的门限群签名方案。所有成员既可以参与签名，也可以作为验证者接收签名，而且份额密钥泄露不会导致签名方案受到攻击。分析表明，该方案具有签名不可伪造性、不诚实签名可识别性、身份可追查性等安全特性，且在运算效率和网络传输量方面具有一定优势。

参 考 文 献

[1] Desmedt Y, Frankel Y. Shared Generation of Authenticators and Signatures(Extended Abstract) [C]// Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology Table of Contents. 1991: 457-469

[2] Tzeng S F, Yang C Y, Hwang M S. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification [J]. Future Generation Computer Systems, 2004, 20(5): 887-893

[3] Hsu C L, Tsai K Y, Tsai P L. Cryptanalysis and improvement of nonrepudiable threshold multi-proxy multi-signature scheme with shared verification [J]. Information Sciences, 2007, 177(2): 543-549

[4] Yang C Y, Tzeng S F, Hwang M S. On the efficiency of nonrepudiable threshold proxy signature scheme with known signers [J]. Journal of Systems and Software, 2004, 73(3): 507-514

[5] Kang B Y, Boyd C, Dawson E. A novel nonrepudiable threshold multi-proxy multi-signature scheme with shared verification [J]. Computers & Electrical Engineering, 2009, 35(1): 9-17

[6] Hong X. Efficient threshold proxy signature protocol for mobile agents [J]. Information Sciences, 2009, 179(24): 4243-4248

[7] Wang C, Chang C, Lin C. Generalization of threshold signature and authenticated encryption for group communications [J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2000, 83(6): 1228-1237

[8] Hsu C L, Wu T S, Wu T C. Improvements of threshold signature and authenticated encryption for group communications [J]. Inform. Process. Lett., 2002, 81(1): 41-45

[9] Chen X F, Zhang F G, Konidala D M, et al. New ID-based threshold signature scheme from bilinear pairings [C]// Proceedings in Progress in Cryptology-Indocrypt. 2004: 371-383

[10] 庞辽军，李慧贤，王育民. 一个(t,n)门限签名-(k,m)门限验证的群签名方案 [J]. 计算机科学，2006，11(33)：76-78

[11] 荆继武，冯登国. 一种入侵容忍的 CA 方案[J]. 软件学报，2002，13(8)：1417-1422