一个预防欺诈的(t, n)门限数字签名方案

庞辽军 谭示崇 王育民
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要：基于离散对数的安全机制，该文提出了一个预防欺诈的 ElGamal 型(t, n)门限数字签名方案。在密钥生成阶段，参与者的公、私钥以及群公钥由所有参与者共同协商而无需可信中心支持；在签名生成阶段，参与者之间不需要进行任何安全通信；能够抵御合法参与者间的相互欺诈和外部攻击者的攻击。方案的安全性是基于离散对数问题的难解性。分析发现，该方案具有良好的安全性和执行效率。

关键词：数字签名；门限数字签名；离散对数；安全性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2007)04-0895-03

A (t, n) Threshold Digital Signature Scheme with Ability to Identify Cheaters

Pang Liao-jun Tan Shi-chong Wang Yu-min
(*State Key Lab. of Integrated Service Networks*, *Xidian Univ.*, *Xi'an* 710071, *China*)

Abstract: Based on the security mechanism of the discrete logarithm, an ElGamal-like (t, n) threshold digital signature scheme with ability to identify cheaters is proposed in this paper. In the key generation phase, each participant's public and private keys, and the group public key are negotiated among all the participants with no trusted party required. In the signature generation phase, no secure communication is needed between any two participants. This scheme provides the capability of detecting cheating and identifying the cheater that may be from the internal legal participants or the external attackers. The security of this scheme is based on the difficulty of solving the discrete logarithm problem. Analyses show that this scheme is a computationally secure and efficient scheme.

Key words: Digital signature; Threshold digital signature; Discrete logarithm; Security

1 引言

数字签名方案的安全性取决于签名密钥，签名密钥的泄漏意味着签名安全性的丧失[1]。通过门限技术，将一个团体的签名密钥以门限方式分散给多人管理，可以分散责任，妥善解决密钥管理中的密钥泄漏和遗失问题，提高了系统的安全性。在一个(t, n)门限签名方案[2]中，只有参与签名的成员数目大于或等于规定的门限值t时才能生成群签名，而任何人都可以利用公开的群公钥来验证群签名的正确性。

目前流行的门限签名方案一般可以分为需要可信中心和不需要可信中心两类。需要可信中心的门限签名方案可以参考文献[3,4]等。由于维护一个可信中心往往会增加系统的实现代价和复杂度，而且在许多特定的应用环境下，一个可被所有小组成员信任的可信中心并不存在，因此不需要可信中心的门限签名方案就显得很有吸引力。文献[5,6]等分别提出了一个不需要可信中心的(t, n)门限签名方案，但签名者之间需要进行秘密通信来交换信息。文献[7]提出了一个基于 Nyberg-Ruepple 方案的不需秘密通信的门限签名方案。本文基于离散对数问题，提出了一个无需可信中心、在签名阶段不需要秘密通信的 ElGamal 型(t, n)门限签名方案。该方案不需要可信中心管理各参与者的密钥，参与者的密钥由所有参与者共同协商；在签名阶段，该方案不需要进行安全通信；同时该方案能够抵御合法参与者之间的相互欺诈和外部攻击者的攻击。因此，该方案具有良好的安全性和执行效率。

2005-08-30 收到，2006-02-24 改回
国家 973 项目(G1999035805)和国家部级基金资助课题

2 方案构成

假设$P=\{P_1, P_2, \cdots, P_n\}$是$n$个参与者的集合。首先，系统中的所有成员需要协商选定公共参数：安全的大素数p和q，以及元素g，其中$q|(p-1)$，并且g在素域Z_p上的阶为q；$h(\cdot)$为一个单向哈希函数[8]。接着，每个成员P_i对外公开自己的唯一标识号ID_i，它可以唯一地代表参与者P_i。

2.1 密钥产生协议

密钥产生协议主要完成各参与者的公钥、私钥以及群公钥的生成。在该过程中，每个参与者$P_i(i=1, 2, \cdots, n)$需要执行如下步骤：

(1) 在$[1, q-1]$中随机选取一个整数d_i。d_i需要安全保护，不能泄漏给其他人。

(2) 随机构造一个$(t-1)$次多项式$f_i(x)=f_{i,0}+f_{i,1}+\cdots$

$+f_{i,t-1}x^{t-1} \bmod q$，其中多项式的系数 $f_{i,0}, f_{i,1}, \cdots, f_{i,t-1}$ 为 Z_q 中的元素，并满足 $f_i(0)= f_{i,0}=d_i$ 且 $f_{i,t-1}\neq 0$。

(3) 对集合P中每一个参与者$P_j(j\neq i)$，计算$f_i(\mathrm{ID}_j)$，并将计算结果安全地发送给P_j。同时，计算多项式系数的公开校验信息 $g^{f_{i,l}} \bmod p$ (l=0,1,…, t–1)，并将其向系统中所有成员广播。

参与者P_j收到P_i发送的$f_i(\mathrm{ID}_j)$后，可以通过下面的等式来验证其有效性：

$$g^{f_i(\mathrm{ID}_j)} = \prod_{l=0}^{t-1} (g^{f_{i,l}})^{(\mathrm{ID}_j)^l} \bmod p \tag{1}$$

如果式(1)成立，那么$f_j(\mathrm{ID}_i)$是有效的；否则是无效的。

(4) 如果P_i已经收到集合P中其他每个参与者P_j ($j\neq i$)如上计算的$f_j(\mathrm{ID}_i)$并验证有效，这时，P_i计算私钥$\mathrm{SK}_i=\sum_{j=1}^{n} f_j(\mathrm{ID}_i) \bmod q$，公钥$\mathrm{PK}_i= g^{\mathrm{SK}_i} \bmod p$，以及群公钥 $\mathrm{GPK}=\prod_{i=1}^{n} g^{f_{i,0}} \bmod p$，并将其公钥和群公钥向系统中所有成员进行广播。

(5) 计算 $\mathrm{PK}_i^{\,d_i} \bmod p$ 以及 $r_i = g^{d_i} \bmod p$ 并将它们向系统中所有成员进行广播。

2.2 个体签名生成协议

不失一般性，选取P中t个参与者P_1，$P_2, \cdots, P_t$为例来说明该协议。每个参与者$P_i(i$=1, 2,…, $t)$需要执行如下步骤：

(1) 在[1, q–1]中随机选取一个整数w_i。然后计算$W_i= g^{w_i} \bmod p$以及$z_i= g^{w_i\cdot(d_i)^{-1}} \bmod p$，其中$d_i$为$P_i$在密钥生成阶段选择的随机数，$(d_i)^{-1}$为$d_i$在素域$Z_q$上的逆元。接着，$P_i$将$W_i$和$z_i$通过广播的方式发送给系统中的其他成员。

(2) 在收到其他参与签名的成员发送的z_i后，P_i计算$r=\prod_{i=1}^{t} z_i \bmod p$，和$s_i=(\mathrm{SK}_i. a_i)\cdot h(m)-r\cdot w_i.(d_i)^{-1} \bmod q$。其中$a_i= \prod_{j=1, j\neq i}^{n} (\mathrm{ID}_j/(\mathrm{ID}_j-\mathrm{ID}_i))$，$m$为要签名的消息，

(3) P_i将$\{r, s_i\}$作为自己对m的签名，并将其发送给指定的群签名生成者。

2.3 群签名生成协议

群签名生成者在收到P_i的个体签名$\{r, s_i\}$时，可以通过验证等式 $r_i^{s_i}\cdot(W_i)^r = (\mathrm{PK}_i^{\,d_i})^{h(m)\cdot a_i} \bmod p$ 是否成立来验证其签名是否有效。如果等式成立，那么P_i的个体签名是正确的；否则无效。当收到t个有效的个体签名$\{r, s_i\}$ (i=1, 2,…, t)后，群签名生成者计算群签名$\{r, s\}$，其中 $s=\sum_{i=1}^{t} s_i \bmod q$。

2.4 群签名验证协议

任何群签名的接收者都可以验证下面的等式是否成立来验证群签名$\{r, s\}$是否有效：

$$g^s r^r = \mathrm{GPK}^{h(m)} \bmod p \tag{2}$$

3 分析和讨论

3.1 正确性分析

接下来我们通过以下定理来分析本文方案的正确性。

定理 1 在密钥产生协议中，参与者P_j能够验证P_i所发送的信息$f_i(\mathrm{ID}_j)$的真伪。

证明 将$x=\mathrm{ID}_j$带入$f_i(x)$可以得到$f_i(\mathrm{ID}_j) = f_{i,0}+\mathrm{ID}_j f_{i,1}+(\mathrm{ID}_j)^2 f_{i,2}+\cdots+(\mathrm{ID}_j)^{t-1} f_{i,t-1}$，进而通过指数运算可以得到式(1)。如果 $g^{f_{i,l}}$ (l=0,1,…, t–1)已知，那么它们就唯一的确定了多项式$f_i(x)$。因此，任何假的信息$f_i'(\mathrm{ID}_j)$都不会使得式(1)的验证成立。可见，该方法能够有效地检测成员之间的相互欺诈或外部攻击者的攻击。 证毕

定理 2 在计算群签名时，签名计算者能够验证合作的参与者P_i的个体签名$\{r, s_i\}$的真伪。

证明 因为z_i (i=0,1,…, t)是公开的，所以签名计算者可以很容易地验证r的正确性。又因为 $r_i^{s_i}(W_i)^r = (g^{d_i})^{(\mathrm{SK}_i\cdot a_i)\cdot h(m)-r\cdot w_i\cdot(d_i)^{-1}} (g^{w_i})^r = (\mathrm{PK}_i^{\,d_i})^{h(m)\cdot a_i} \bmod p$，等式两边的信息都是公开的或利用公开信息可计算的，所以通过验证等式 $r_i^{s_i}\cdot(W_i)^r = (\mathrm{PK}_i^{\,d_i})^{h(m)\cdot a_i} \bmod p$ 是否成立就可以验证s_i是否有效。 证毕

定理 3 在群签名验证中，如果等式 $g^s r^r = \mathrm{GPK}^{h(m)} \bmod p$ 成立，那么$\{r, s\}$是 m 的有效签名。

证明 首先

$$g^s r^r = g^{\sum_{i=1}^{t} s_i} \cdot g^{r\sum_{i=1}^{t} w_i\cdot(d_i)^{-1}} = g^{\sum_{i=1}^{t}((\mathrm{SK}_i\cdot a_i)\cdot h(m)-r\cdot w_i\cdot(d_i)^{-1})} \cdot g^{r\sum_{i=1}^{t} w_i\cdot(d_i)^{-1}} = g^{\sum_{i=1}^{t}(\mathrm{SK}_i\cdot a_i)\cdot h(m)}$$

因为$a_i= \prod_{j=1, j\neq i}^{n} (\mathrm{ID}_j/(\mathrm{ID}_j-\mathrm{ID}_i))$ 和$\mathrm{SK}_i=\sum_{j=1}^{n} f_j(\mathrm{ID}_i)$，所以有

$$g^s r^r = g^{\sum_{i=1}^{t}(\mathrm{SK}_i\cdot a_i)\cdot h(m)} = g^{h(m)\cdot\sum_{i=1}^{t}(\sum_{k=1}^{n} f_k(\mathrm{ID}_i)\cdot\prod_{j=1, j\neq i}^{n}(\mathrm{ID}_j/(\mathrm{ID}_j-\mathrm{ID}_i)))} = g^{h(m)\cdot\sum_{k=1}^{n}(\sum_{i=1}^{t} f_k(\mathrm{ID}_i)\cdot\prod_{j=1, j\neq i}^{n}(\mathrm{ID}_j/(\mathrm{ID}_j-\mathrm{ID}_i)))} \bmod p$$

根据Lagrange插值定理或者Shamir的门限体制[9]，(t–1)多项式$f(x)$上任意t个点$(X_i,\ Y_i)$ (i=1, 2,…, t)可以唯一地确定$f(x)$：$f(x)=\sum_{i=1}^{t} Y_i \prod_{j=1, j\neq i}^{n} \frac{x-X_j}{X_i-X_j}$。同理，$t$个点$(\mathrm{ID}_i, f_k(\mathrm{ID}_i))$可以唯一地确定方程$f_k(x)$(见 2.1 节)，因此有 $\sum_{i=1}^{t} f_k(\mathrm{ID}_i) \cdot \prod_{j\in P, j\neq i} (\mathrm{ID}_j/(\mathrm{ID}_j-\mathrm{ID}_i)) = f_k(0)= f_{k,0}$。从而可得到：

$$g^s r^r = g^{h(m)\cdot\sum_{k=1}^{n} f_{k,0}} = \left(\prod_{i=1}^{n} g^{f_{i,0}}\right)^{h(m)} = \mathrm{GPK}^{h(m)} \bmod p \text{。} \quad \text{证毕}$$

3.2 安全性分析

本文方案的安全性是基于离散对数问题的难解性，它主要会面临以下方面的攻击。下面通过对这些攻击进行分析来

说明本文方案的安全性。

攻击 1　在密钥生成协议中，一个参与者P_i可能会发送给其他参与者$P_j(i\neq j)$一个假的信息$f_i'(\mathrm{ID}_j)$，来试图欺骗P_j而不被发现。

分析：任何面向群的密码方案都应该具备防欺骗能力[10]。由定理 1 可知，可以使用式(1)来验证$f_i'(\mathrm{ID}_j)$。如果$g^{f_{i,l}}$ (l=0,1,…, t–1)已知，那么它们就唯一地确定了多项式$f_i(x)$。因此，任何假的信息$f_i'(\mathrm{ID}_j)$都不会使得式(1)的验证成立。

攻击 2　在计算签名时，参与者P_i可能会提供假的个体签名$\{r, s_i\}$来欺骗群签名计算者。

分析：由定理 2 可知，群签名计算者可以通过验证等式$r_i^{s_i}\cdot(W_i)^r=(\mathrm{PK}_i^{d_i})^{h(m)\cdot a_i} \bmod p$ 是否成立来验证P_i提交的个体签名$\{r, s_i\}$的真伪。由于除s_i外其他的信息都是公开的或可直接利用公开信息计算的，因此，要找到一个假的s_i并满足等式是不可行的。故，该攻击无法奏效。

攻击 3　攻击者试图由参与者P_i的公钥PK_i来推导他的私钥SK_i。

分析：攻击者由P_i的公钥PK_i来推导他的私钥SK_i将面临求解离散对数问题的困难性。而且在密钥生成阶段，参与者之间使用的都是安全信道，因此，该攻击无法奏效。

攻击 4　在个体签名产生阶段，攻击者试图冒充某个参与者P_i伪造其个体签名。

分析：由攻击 3 的分析可知，攻击者无法得到参与者P_i的私钥SK_i。攻击者为了伪造P_i的个体签名，首先必须选择一个随机数w_i'使得 $1\leqslant w_i'\leqslant q-1$，然后计算并广播$W_i'=g^{w_i'} \bmod p$。这时，他面临着计算一个$s_i'$并满足$r_i^{s_i'}\cdot(W_i')^r=(\mathrm{PK}_i^{d_i})^{h(m)\cdot a_i} \bmod p$ 的困难性，即求解离散对数问题的困难性。根据攻击 2 的分析可知，假的个体签名不能通过群签名计算者的验证。

攻击 5　攻击者试图通过获得一个合法群签名来为自己选定的一条消息伪造一个合法群签名。

分析：假设一个攻击者已获得消息m的合法群签名$\{r, s\}$，并选定一条消息m'。注意到r_i (i=1, 2,…, n)是固定的，我们分析一下攻击者是否有可能伪造一个合法群签名$\{r', s'\}$。因为$s=\sum_{i=1}^{t}s_i=\sum_{i=1}^{t}((SK_i\cdot a_i)h(m)-rw_i(d_i)^{-1}) \bmod q$，在其两端同时乘以$h^{-1}(m)\cdot h(m')$，可以得到：$h^{-1}(m)\cdot h(m')\cdot s=\sum_{i=1}^{t}(\mathrm{SK}_i\cdot a_i)\cdot h^{-1}(m)-h^{-1}(m)\cdot h(m')\cdot r\sum_{i=1}^{t}w_i\cdot(d_i)^{-1} \bmod q$。令$h^{-1}(m)\cdot h(m')\cdot s=s'$，要使式(2)验证成立，攻击者需要根据下面的等式

$$g^{\sum_{i=1}^{t}(\mathrm{SK}_i\cdot a_i)h^{-1}(m)-h^{-1}(m)\cdot h(m')\cdot r\sum_{i=1}^{t}w_i\cdot(d_i)^{-1}}r^{r'}=\mathrm{GPK}^{h(m')} \bmod p$$

求出 r'。而式中的$\sum_{i=1}^{t}w_i\cdot(d_i)^{-1}$对攻击者来说是未知的，因此攻击者只能够通过猜测来求取一个满足上面等式的 r'。这在计算上是不可行的，故该攻击无法奏效。

4　结束语

本文提出了一个基于离散对数问题的 ElGamal 型(t, n)门限群签名方案，并对该方案的正确性和安全性进行了分析。分析表明，该方案在密钥生成阶段不需要可信中心；在签名阶段，该方案不需要进行安全通信；同时该方案能够抵御参与者的相互欺诈和外部攻击者的攻击。因此，该方案具有良好的安全性和执行效率。

参 考 文 献

[1] Mehta M and Harn L. Efficient one-time proxy signatures. *IEE Proceedings-Communications*, 2005, 152(2): 129–133.

[2] Rosario G, Stanislaw J, and Hugo K. Robust threshold DSS signatures. *Information and Computation*, 2001, 164(1): 54–84.

[3] Wang C T, Lin C H, and Chang C C. Threshold signature schemes with traceable signers in group communications. *Computer Communications*, 1998, 21(8): 771–776.

[4] 许春香, 董庆宽, 肖国镇. 矢量空间秘密共享——多重签名方案.电子学报, 2003, 31(1): 48–50.

[5] Miyazaki K and Takaragi K. A threshold digital signature scheme for a smart card based system. *IEICE Trans. Fundamentals*, 2001, E84-A(1): 205–213.

[6] Chang Ting-Yi, Yang Chou-Chen, and Hwang Min-Shiang. A threshold signature scheme for group communications without a shared distribution center. *Future Generation Computer Systems*, 2004, 20(6): 1013–1021.

[7] Takaragi K, Miyazaki K, and Takahashi M, *et al.*. A threshold digital signature issuing scheme without secret communication. http://grouper.ieee.org/groups/1363/StudyGroup/contributions/th-sche.pdf, 2002-12-01.

[8] Vandierendonck H and De Bosschere K. XOR-based hash functions. *IEEE Tran. on Computers*, 2005, 54(7): 800–812.

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

[10] Wang Shiuh-Jeng. Direct construction of a secret in generalized group-oriented cryptography. *Computer Standards and Interfaces*, 2004, 26(5): 455–460.

庞辽军：　男，1978年生，博士生，研究方向为电子商务中的安全理论与技术.

谭示崇：　男，1979年生，博士生，研究方向为公钥密码学及其应用.

王育民：　男，1936年生，博士生导师，主要从事编码理论、密码学、信息安全等领域的科研与教学工作.