一种安全的门限盲签名方案①

胡建军

(甘肃联合大学 电子信息工程学院，兰州 730000)

摘　要：门限签名在电子签名中有着广泛的应用，针对客户端运行能力的不足，结合双线性映射、门限身份、门限盲签名，提出了一种高效安全的门限签名方案。分析表明，方案易于实现，系统的安全性更高，能够满足电子门限签名的需求。

关键词：门限签名；门限身份；盲因子；双线性映射

Security Signature Scheme of Threshold and Blindness

HU Jian-Jun

(College of Electric and Information Engineering, Gansu Lianhe University, Lanzhou 730000, China)

Abstract: The threshold signature is popular in electronic signature. This paper presents an efficient secure threshold signature scheme on threshold, which uses bilinear paring, threshold identity, and threshold blinding signature to solve deficiency about client performance. Analysis shows that the scheme is easy to realize and the safety of system is high. The scheme can satisfy the demand of electronic signature.

Key words: threshold signature; threshold identity; blindness gene; bilinear mapping

在现代密码学研究中，签名占有十分重要的地位，而以群体签名为主要形式的门限签名[1-3]，是现代密码学研究的重要方向之一。以公钥为基础的门限签名算法（以下简称门限签名算法）可以分成两类，一类建立在求解离散对数的困难性上，另一类建立在大整数分解的困难性上，而以第一类为基础开展研究者居多。在第一类研究中，又可以分两类，一类以椭圆曲线为基础，另一类以 Elgamal 体制为基础。

消息的拥有者有时只想他人证实该消息的存在，不希望他人了解消息的具体内容,另外签名者无需关心消息的内容,因而盲签名的概念便应运而生[4]。当签名出现纠纷时需要追查消息的签名者，文献[5-6]提出一种基于身份的签名方案，文献[7]将身份、门限、盲签名结合起来提出一种基于身份的门限盲签名方案。以上方案各有所长，但都存在运算过程复杂、客户端性能要求高等缺陷，为此，本文提出一种基于身份的门限盲签名方案，该方案运行效率、安全性和可扩展性更好。

1　相关知识

1.1 双线性映射

设 G_1 和 G_2 分别是阶为大素数 q 的加法群和乘法群，P 为 G_1 的生成元。假设 G_1 和 G_2 的离散对数问题都是困难问题，则映射 $e: G_1 \times G_1 \to G_2$ 称为双线性映射。e 具有如下的特性：

(1) 双线性性：$\forall P,Q \in G_1, a,b \in Z$，有 $e(aP,bQ)=e(P,abQ)=e(P,Q)^{ab}$。

(2) 非退化性：$\exists P \in G_1$，满足 $e(P,P) \neq 1$。

(3) 可计算性：对 $\forall P,Q \in G_1$，存在有效算法计算 $e(P,Q)$。

1.2 与双线性映射有关的几个密码学问题

(1) 离散对数问题（DLP）：对于 $\forall P,Q \in G_1$，已知 $Q=nP$，则通过 Q 和 P 求解 n 是困难的。

(2) 判定 Diffie-Hellman 问题（DDHP）：对于 $\forall P \in G_1$，$a,b,c \in Z_q^*$，给定 P，aP，bP，cP，判定 $c \equiv ab \pmod q$ 是困难的。

(3) 计算 Diffie-Hellman 问题(CDHP)：对于

① 收稿时间:2011-09-06;收到修改稿时间:2011-11-14

$a,b\in Z_q^*$，$\forall P\in G_1$，给定 P，aP，bP，计算 abP 是苦难的。

(4) 间隙 Diffie-Hellman 问题（GDHP）：当群 G_1 上的 DDHP 是容易的而计算 CDHP 是困难的。

2 基于身份的门限盲签名方案

2.1 签名方案

方案由群用户、签名机构和可信中心三部分组成，群用户负责门限签名的申请、签名，签名机构负责门限签名的许可、请求与验证，可信中心负责群用户身份的生成、密钥的生成以及对门限签名的违规追查，三者之间的关系如图 1 所示：

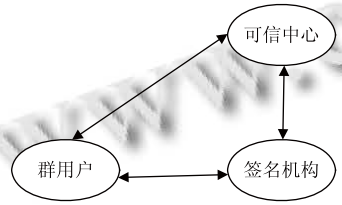

图 1 签名方案

2.2 用户身份、密钥的生成与获取

(1) 系统初始化：可信中心向群用户共享并发布公共系统参数 $\{G_1,G_2,e,P,H,t\}$，其中 G_1、G_2 阶为大素数 q 的循环群，P 是群 G_1 的生成元，e 为双线性映射，定义为 $e:G_1\times G_1\to G_2$，H 为哈希函数，定义为 $H:\{0,1\}^*\to G_1$，t 为门限。

(2) 身份、密钥的生成：可信中心选择两个 $t-1$ 次多项式，即 $f(x)=s+\sum_{i=1}^{t-1}a_ix^i \pmod q$ 和 $g(x)=k+\sum_{i=1}^{t-1}b_ix^i \pmod q$，其中 $f(x)$ 用于生成群用户身份，$g(x)$ 用于生成群用户密钥，显然 $f(0)=s$ 为群身份，$g(0)=k$ 为群私钥。并按下列步骤生成群用户身份与密钥：

① 计算成员份额 $ID_i=f(x_i),x_i\in Z_q$，其中对于 $\forall x_i,x_j\in Z_q,x_i\neq x_j$。

② 计算密钥份额 $Q_i=g(x_i)P$，其中对于 $\forall x_i,x_j\in Z_q,x_i\neq x_j$。

(3) 身份、密钥的分发：可信中心通过安全信道将 x_i 和 $g(x_i)$ 秘密发送给用户，并将 ID_i 和 Q_i 向群用户共享。

(4) 签名机构授权：签名机构按照下列步骤获得授权：

① 签名机构利用自己的身份 ID 向可信中心注册，可信中心存储 ID。

② 可信中心计算 $ID_T=f(x_T)+ID,x_T\in Z_q$，$y_T=g(x_T)$，$Q_T=(y_T+ID)P$，将 x_T、y_T 通过安全信道秘密发送给签名机构，并公开签名机构的身份和公钥。

2.3 门限签名

一个正确的门限签名需要完成下列步骤：

(1) 签名申请：签名用户发送信息 $(M_1,rP,ID_uH(M))$ 给签名机构，其中随机数 $\forall r\in Z_q$，$M_1=H(M)+rQ_T$，M 为要签名的消息，Q_T 为签名机构的公开群密钥份额。

(2) 签名机构签名：签名机构计算并判断 $ID_u[M_1-(y_T+ID)rP]\stackrel{?}{\equiv}ID_uH(M)$ 是否成立，若成立，则认为申请合法，接受请求，并向 $t-1$ 个群用户发送消息 $M_2=M_1-(ID+y_T)rP+rp$ 请求签名。每一个签名者签名并返回消息 $\{r_ig(x_i)M_2,r_ig(x_i)P\}$，其中 $\forall r_i\in Z_q$，当签名机构成功接收 $t-1$ 个群用户的签名之后，计算 $M_3=\sum_{i=1}^{t-1}g(x_i)M_2$，$M_4=\sum_{i=1}^{t-1}r_ig(x_i)P$，并将消息 $\{M_3,M_4\}$ 及群用户签名列表返回签名申请者。

(3) 申请签名者去盲化并签名。$M_5=(M_3-rM_4)+rg(x_u)H(M)$，$M_5$ 为门限签名消息，即 $\sum_{i=1}^{t}r_ig(x_i)H(M)$，$g(x_u)$ 为签名申请者自己的私钥。

2.4 无效门限签名的追查

如果签名失败，签名申请者可向可信中心提出申请，由可信中心追查不良的签名，由于可信中心存储着所有群用户的身份、私钥、公开信息，所以，只要请求签名者能够提供签名用户的列表信息，就可以追查出包括签名机构在内的不良签名者。

3 性能分析

3.1 安全性分析

本文方案具有如下性质：

(1) 盲性。由于签名申请者选择的$\forall r \in Z_q$是随机的，而且$H(\gamma)$是单向散列的，其他用户不可能获得信息M，因此签名保证了消息的盲性。

(2) 可追查性。由于本方案中签名仲裁是由可信中心完成的，因此如果签名是正确的，那么，群用户的身份是可追查的。

(3) 门限签名特性。因为可信中心可以通过t个用户的密钥信息可求出

$g(x)=\sum_{j=1}^{t} g(x_j)\prod_{i=1,\ i\neq j}^{t}\frac{x-x_i}{x_j-x_i}$，而$g(0)=k$，另外可以通过$t$个用户的身份求出$f(x)=\sum_{j=1}^{t} f(x_j)\prod_{i=1,\ i\neq j}^{t}\frac{x-x_i}{x_j-x_i}$，而$f(0)=s$，所以方案具有门限签名特性。

(4) 防伪造性。可以分三种情形讨论。

① 普通用户伪造普通用户。很显然，伪造签名是不可能的，这是因为，假设群用户A要冒充B签名，由于A没有B的私钥而使伪造签名失败。

② 普通用户伪造签名机构。由于普通用户无法获取签名机构的私钥y_T，因此他无法rQ_T将替换成消息rP，即将消息M_1替换成消息M_2，从而伪造签名机构失败。

③ 签名机构伪造普通用户。假设签名机构要冒充普通用户B签名，由于签名机构不可能获得普通用户B的私钥和盲签名因子，因而伪造签名失败。

综上所述，方案是防伪造的。

(5) 抗合谋性。如果有t个以上的群用户想要合谋获取M，则合谋失败。这是因为，$H(\gamma)$是单向散列的，而且，签名申请者的私钥$x_i \in Z_q$是随机的，因此如果合谋攻击成功，则必须能够求出$H(\gamma)$的逆，这是不可能的。

(6) 验证简单。检查双线性映射的正确性，即等式$e(\sum_{i=1}^{t-1} r_i g(x_i)P, rP)=e(r\sum_{i=1}^{t-1} g(x_i)P, P)$成立，签名合法，验证通过。

3.2 运行效率分析

由于签名的合成是由签名机构完成的，除签名申请者外，普通用户不再负担验证任务，只需签名即可。另外，签名申请者不再去判断谁能够签名，也不去验证普通用户签名的正确性，此任务均由签名机构完成，这样一来，对客户端的性能要求就会降低。文献[1-7]所有的客户端要承担签名验证和判断谁能够实现签名，有些方案客户端还要承担签名合成任务。

尽管此方案增加了签名机构的负担，但是由于签名合成是必不可少的，因而，把签名验证和合成交给签名机构是合理的。

4 结语

结合双线性映射、门限身份、门限盲签名，提出一个高效安全的门限签名方案。该方案通过签名机构完成$t-1$个群用户的签名，防止了群用户之间的合谋攻击，通过可信中心的裁决，能够追查签名者的不良行为。由于客户端仅需少量的计算，因此方案对于提高客户端运行效率和减轻客户端维护成本具有重要的意义。

参考文献

1 Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. Proc. Of CRYPTO'91. Berlin, Germany: Springer-Verlag, 1992.

2 Desmedt Y, Frankel Y. Threshold cryptosystems. Brassard G, ed. Proc. of the Crypto'89. LNCS 435, Berlin: Springer-Verlag, 1990: 307–315.

3 Desmedt Y, Frankel Y. Shared generation of authentications and signatures. Desmedt Y, Frankel Y, eds. Advances in Cryptology-Crypto'91. LNCS, Berlin: Springer-Verlag, 1992: 457–469.

4 Chaum D.Blind Signatures for untaceable payments. http://citeseer.ist.psu.edu/cotext/2064/0.html(2000-06-25).

5 Boneh D, Franklin MK. Identity based encryption from the weil pairing. SIAM Journal on Computing, 2003,32(3):586–615.

6 Mihir B, Chanathip N, Neven G. Security proofs for identity-based identification and signature schemes. Proc. of the Eurocrypt 2004. Berlin, Germany: Springer-Verlag, 2004.

7 涂峰,赵一鸣.一种基于身份的门限盲签名方案.计算机工程,2008,34(21):118–119.