鲁棒的多重代理多重盲签名方案

田娟红,张建中,李艳平
TIAN Juanhong, ZHANG Jianzhong, LI Yanping

陕西师范大学 数学与信息科学学院,西安 710119
College of Mathematics & Information Science, Shaanxi Normal University, Xi'an 710119, China

TIAN Juanhong, ZHANG Jianzhong, LI Yanping. Robust multi-proxy multi-blind signature scheme. Computer Engineering and Applications, 2017, 53(1):130-133.

Abstract: A multi-proxy multi-signature scheme requires all proxy signers to participate in the signature, and some proxy signers' absence will lead to the proxy signature's failure, and the proxy signers who participate in the signature will know the concrete content of the message. So there exist security flaws. Based on the threshold signature and blind signature, the paper proposes a (t,n) robust multi-proxy multi-blind signature scheme. In this scheme, any t (or more than t) proxy signers can generate a signature of a specific message, and they don't know the concrete content of the message so as to avoid the exposure of the sensitive information. At last, the message owner will remove the blind factor and finish the final signature. The security analysis shows that the scheme satisfies the security features of unforgeability, undeniability, traceability, robustness and unlinkability etc.

Keywords: discrete logarithm problem; proxy signature; threshold signature; blind signature; robustness

摘 要: 多重代理多重签名方案要求所有代理签名人参与签名,若其中一个代理签名人缺席就会导致无法进行代理签名,且参与签名的代理人均知晓消息内容,存在安全缺陷。结合门限签名和盲签名,提出一个 (t,n) 门限多重代理多重盲签名,只要 t 个(或 t 个以上)代理签名人就能对消息签名,且代理签名人对消息不知情,避免了敏感信息的暴露,最后消息拥有者进行脱盲变换完成最终签名。经安全性分析证明该方案满足不可伪造性、不可否认性、可追踪性、鲁棒性和不可链接性等安全特性。

关键词: 离散对数困难性问题;代理签名;门限签名;盲签名;鲁棒性
文献标志码: A **中图分类号:** TP309 doi:10.3778/j.issn.1002-8331.1503-0294

1 引言

代理签名[1]于1996年由Mambo、Usuda和Okamoto提出,允许原始签名人将签名权委托给代理签名人生成有效的代理签名。随后为满足实际需求,代理多重签名[2-3]($m\rightarrow 1$,m 个原始签名人将签名权委托给一个代理签名人)、多重代理签名[4]($1\rightarrow n$,一个原始签名人将签名权委托给 n 个代理签名人)、多重代理多重签名[5]($m\rightarrow n$,m 个原始签名人将签名权委托给 n 个代理签名人)随即被提出,而且多重代理多重签名是 $m\rightarrow 1$ 和 $1\rightarrow n$ 应用的扩展,增加了方案的灵活性。Kim[6]与Zhang[7]等人分别独立地构造了最初的门限代理签名方案,它是对代理签名方案的一种改进。在一个 (t,n) 门限代理签名方案中,一个原始签名人将签名权委托给 n 个代理签名人,使其中 t 个(或 t 个以上)代理签名人合作就能产生有效的代理签名,此后出现了大量的门限代理签名方案[8-11]。盲签名是Chaum[12]提出的对盲化消息的一种签名,即签名人看不到自己所签署消息的具体内容,且消息拥有者在公布消息的签名后,签名者不能将

基金项目: 国家自然科学基金(No.61402275,No.61273311,No.61173190);陕西省自然科学基金(No.2015JM6263);陕西省自然科学基础研究计划项目(No.2012JQ8023);中央高校基本科研业务费专项基金(No.GK201402004)。

作者简介: 田娟红(1989—),女,硕士研究生,主要研究方向为密码学,E-mail:tjh@snnu.edu.cn;张建中(1960—),通讯作者,男,教授,主要研究方向为密码学与信息安全;李艳平(1978—),女,副教授,主要研究方向为密码学与信息安全。

收稿日期: 2015-03-26 **修回日期:** 2015-06-04 **文章编号:** 1002-8331(2017)01-0130-04
CNKI网络优先出版: 2015-09-14, http://www.cnki.net/kcms/detail/11.2127.TP.20150914.1650.048.html

签名过程与公布的签名联系起来,从而无法实现对消息拥有者的追踪,从而保护了消息拥有者的隐私。

文献[13]指出李传目的多重代理多重签名[5]方案易受恶意代理签名人的伪造攻击,并对此方案做出改进,同时增加了许多新的特性,如撤销代理签名管理人等。2010年,在文献[14]中,指出文献[13]方案中存在的安全漏洞,如易出现滥用签名权等安全缺陷,并做出改进。文献[15]则基于这些方案,改进了签名过程,具有更好的安全特性。但这几个方案[5,13-15]都有共同不足之处:(1)只要有一个代理签名人因为某些原因缺席而不能亲自签名,或者计算出错,就会导致该多重代理多重签名方案彻底失败;(2)消息对于代理签名人来说是完全公开透明的,当消息拥有者不希望签名人知晓消息内容时,此类方案的应用就受限了。此外,方案[5,13-15]中关于证书的构造较繁琐,本文针对这几点缺陷,提出了一个基于离散对数的高效的鲁棒的多重代理多重盲签名方案。本文方案可适用于以下场合:在一个大公司中,有多个副董事长和部门经理。由于某些副董事长出国休假或身体有恙,所有副董事长便可将签名权委托给多个部门经理,当董事长要求所有副董事长对一个机密文件进行签名时,只需部分经理就可以代替所有副董事长完成签名,且参与签名的部门经理对所签署机密文件的内容也不知情。

2 鲁棒的多重代理多重盲签名方案

2.1 系统参数与符号说明

方案的系统参数:p 和 q 为大素数,其中 q 为 $p-1$ 的大素因子,$g\in Z_p^*$ 且满足 $g^q\equiv 1(\mathrm{mod}\,p)$,$h(\cdot)$ 是一个安全的单向哈希函数,$\|$ 表示比特串的级联。假设 Z_p 上离散对数问题是困难的,且小于 t(t 为门限值)个代理签名人可以不诚实,即不忠实地执行协议。

方案的符号说明:原始签名人 $U_i(i=1,2,\cdots,m)$ 的私钥 $x_{U_i}\in Z_q^*$,公钥 $y_{U_i}=g^{x_{U_i}}\bmod p$;代理签名人 $P_j(j=1,2,\cdots,n)$ 的私钥 $x_{P_j}\in Z_q^*$,公钥 $y_{P_j}=g^{x_{P_j}}\bmod p$,身份信息 ID_j;U_I 为消息拥有者。

2.2 代理证书生成阶段

假设 m 个原始签名人和 n 个代理签名人对代理签名的消息范围及代理有效期限进行协商和约定,形成委托代理签名协议 W(其中包括所有原始签名人和代理签名人的公钥)。

(1) U_i 随机选择 $k_{U_i}\in Z_q^*$,计算 $L_{U_i}=g^{k_{U_i}}\bmod p$,发给其他 $m-1$ 个原始签名人和 n 个代理签名人;每个 P_j 随机选择 $k_{P_j}\in Z_q^*$,计算 $L_{P_j}=g^{k_{P_j}}\bmod p$,发给其他 $n-1$ 个代理签名人和 m 个原始签名人。最后,所有原始签名人和代理签名人计算并保存 $K=\prod_{i=1}^{m}L_{U_i}\prod_{j=1}^{n}L_{P_j}\bmod p$。

(2) U_i 计算 $V_{U_i}=(h(W)x_{U_i}+k_{U_i}K)\bmod q$,发给其他 $m-1$ 个原始签名人和 n 个代理签名人,则 U_i 的个人委托证书为 (L_{U_i},V_{U_i});P_j 计算 $V_{P_j}=(h(W)x_{P_j}+k_{P_j}K)\bmod q$,发给其他 $n-1$ 个代理签名人和 m 个原始签名人,则 P_j 的个人代理证书为 (L_{P_j},V_{P_j})。

(3)每个 U_i/P_j 通过式(1)、(2)验证 V_{U_i}/V_{P_j} 的正确性:

$$g^{V_{U_i}}=y_{U_i}^{h(W)}L_{U_i}^{K}\bmod p,\ i=1,2,\cdots,m \tag{1}$$

$$g^{V_{P_j}}=y_{P_j}^{h(W)}L_{P_j}^{K}\bmod p,\ j=1,2,\cdots,n \tag{2}$$

若 V_{U_i} 和 V_{P_j} 都正确,则每个代理签名人 P_j 计算 $V=(\sum_{i=1}^{m}V_{U_i}+\sum_{j=1}^{n}V_{P_j})\bmod q$,生成委托代理证书 (K,V)。

2.3 代理签名密钥生成阶段

(1)每个 P_j 随机选择 $n_j\in Z_q^*$,计算并广播 $N_j=g^{n_j}\bmod p$,要求代理签名人中任意 t 个 N_j 之积 $\prod_{j=1}^{t}N_j\bmod p$ 互不相等(为使签名具有可追踪性,以抵抗合谋攻击[16])。

(2)每个 P_j 随机选择 $a_{je}\in Z_q^*(e=1,2,\cdots,t-1)$,计算并将 $g^{a_{je}}\bmod p$ 广播给其他代理签名人。构造一个 $t-1$ 次多项式 $f_j(x)=\sum_{e=0}^{t-1}a_{je}x^e\bmod q$,满足 $a_{j0}=(x_{P_j}+n_jV)\bmod q$。$P_j$ 为其他 $P_i(i=1,2,\cdots,n,i\neq j)$ 计算并发送子秘密 $f_j(ID_i)\bmod q$,计算并保存 $f_j(ID_j)\bmod q$。

(3)每个 P_i 收到 $f_j(ID_i)\bmod q$ 后验证式(3)是否成立。

$$g^{f_j(ID_i)}=y_{P_j}N_j^{V}\prod_{e=1}^{t-1}g^{a_{je}(ID_j)^e}\bmod p \tag{3}$$

若不成立,要求重新发送;反之,P_i 接受秘密份额,并计算代理签名密钥 $c_i=\sum_{j=1}^{n}f_j(ID_i)\bmod q$,公开 $C_i=g^{c_i}\bmod p$。

2.4 代理签名生成阶段

设待签消息为 M,n 个代理签名人中任意 t 个 $(P_1,P_2,\cdots,P_t)$ 构成集合 E,令 $N=\prod_{j=1}^{t}N_j\bmod p$。签名流程图如图1所示,具体签名过程如下:

(1)每个 $P_i\in E$ 随机选择 $r_i\in Z_q^*$,计算 B_i 并发给 U_I。

(2) U_I 计算 B,随机选择 $\alpha,\beta\in Z_q^*$ 对消息 M 进行盲化,计算 B' 和 $\bar{M}$,并将 B 和 $\bar{M}$ 发送给 E 中成员。

(3) E 中每个代理签名人 P_i 计算并将部分签名 S'_i 发给消息拥有者 U_I,其中 $T_i=\prod_{j=1,j\neq i}^{n}\frac{-ID_j}{ID_i-ID_j}\bmod q$。

(4) U_I 收到 S'_i 后验证式(4)是否成立。

$$g^{S'_i}=(C_i^{T_i}N_i^{N})^{(B+\bar{M}h(W))}\bmod p \tag{4}$$

若不成立,要求重新发送;反之,计算 S' 和进行脱盲变换 $S=\alpha S'\bmod q$,得到消息 M 的最终签名 (N,B',S)。

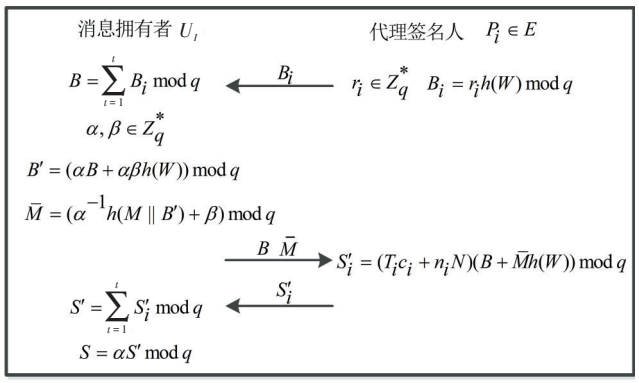

图1　代理签名生成流程

2.5　代理签名验证阶段

任何知晓 M 者结合2.2节生成的委托代理证书 (K,V) 均可对最终签名 (N,B',S) 的有效性进行验证，其中 $Y=\prod_{i=1}^{n} y_{P_i} \bmod p$，$Q=\prod_{i=1}^{n} N_i \bmod p$。验证式如下：

$$g^V = K^K\left(\prod_{i=1}^{m} y_{U_i}\prod_{j=1}^{n} y_{P_j}\right)^{h(W)} \bmod p \tag{5}$$

$$g^S = (YQ^V N^N)^{B'+h(M\|B')h(W)} \bmod p \tag{6}$$

3　方案分析

3.1　正确性证明

定理1 若原始签名人和代理签名人严格按照2.2节中的(1)、(2)生成正确参数，则式(1)、(2)可通过验证。

证明 $g^{V_{U_i}} = g^{h(W)x_{U_i}+k_{U_i}K} = y_{U_i}^{h(W)} L_{U_i}^K \bmod p$，即式(1)可通过验证，同理可证式(2)可通过验证。原始签名人和代理签名人通过验证式(1)、(2)成立，确认他们的个人委托证书和个人代理证书的安全性。

定理2 若代理签名人 P_j 严格按照2.3节(1)、(2)生成正确参数，则式(3)可通过验证。

证明 $g^{f_j(ID_i)} = g^{(x_{P_j}+n_j V)} g^{\sum_{e=1}^{t-1} a_{je}(ID_i)^e} = y_{P_j} N_j^V \prod_{e=1}^{t-1} g^{a_{je}(ID_i)^e} \bmod p$，$P_j$ 通过验证式(3)成立，确认秘密份额的有效性。

定理3 若消息拥有者 U_I 和 E 中成员严格按照2.4节(1)~(3)生成正确参数，则式(4)可通过验证。

证明 $g^{S'_i} = g^{(T_i c_i+n_i N)(B+\bar{M}h(W))} = (C_i^{T_i} N_i^N)^{(B+\bar{M}h(W))} \bmod p$，$U_I$ 通过验证式(4)成立，确认 S'_i 的有效性。

定理4 若原始签名人，代理签名人和消息拥有者严格按照方案2.2~2.4节步骤生成正确参数，则式(5)、(6)可通过验证。

证明 下证式(5)成立：

$$g^V = g^{\sum_{i=1}^{m}(h(W)x_{U_i}+k_{U_i}K)} g^{\sum_{j=1}^{n}(h(W)x_{P_j}+k_{P_j}K)} = g^{(\sum_{i=1}^{m}k_{U_i}+\sum_{j=1}^{n}k_{P_j})K} g^{(\sum_{i=1}^{m}x_{U_i}+\sum_{j=1}^{n}x_{P_j})h(W)} = K^K\left(\prod_{i=1}^{m} y_{U_i}\prod_{j=1}^{n} y_{P_j}\right)^{h(W)} \bmod p$$

证式(6)成立：因为 $\sum_{i=1}^{t} T_i c_i = \sum_{i=1}^{n} f_i(0) = \sum_{i=1}^{n}(x_{P_i}+n_i V) \bmod q$，所以

$$g^S = \left(g^{\sum_{i=1}^{t} T_i c_i} g^{\sum_{i=1}^{t} n_i N}\right)^{\alpha B+\alpha(\alpha^{-1}h(M\|B')+\beta)h(W)} = \left(\prod_{i=1}^{n} y_{P_i}\prod_{i=1}^{n} N_i^V N^N\right)^{\alpha B+\alpha\beta h(W)+h(M\|B')h(W)} = (YQ^V N^N)^{B'+h(M\|B')h(W)} \bmod p$$

任何知晓 M 者通过验证式(5)、(6)成立，来确认最终签名 (N,B',S) 的有效性。

3.2　安全性证明

(1)证书的安全性

定理5 在DLP(离散对数问题)困难性假设下，U_i 的个人委托证书 (L_{U_i},V_{U_i})，P_j 的个人代理证书 (L_{P_j},V_{P_j}) 和委托代理证书 (K,V) 是安全的。

证明 设攻击者A伪造 U_1 的证书为 (L_{U_1}',V_{U_1}')，需满足式：$g^{V_{U_1}'} = y_{U_1}^{h(W)} L_{U_1}'^{K'} \bmod p$，$K'=L_{U_1}'\prod_{i=2}^{m} L_{U_i}\prod_{j=1}^{n} L_{P_j} \bmod p$. 设已知 L_{U_1}'，通过上述两式求解 V_{U_1}'，需求解 Z_p 上离散对数，因此 U_1 的个人委托证书是安全的，同理可证 P_j 的证书 (L_{P_j},V_{P_j}) 是安全的。

设A伪造委托代理证书 (K',V')，需满足式：$g^{V'} = K'^{K'}\left(\prod_{i=1}^{m} y_{U_i}\prod_{j=1}^{n} y_{P_j}\right)^{h(W)} \bmod p$，在DLP困难性假设下，$(K,V)$ 的安全性得证。

(2)不可伪造性

代理签名的存在性不可伪造[17-18]分为存在性授权不可伪造性和代理签名存在性不可伪造性：① 存在性授权不可伪造性，由证书安全性分析表明，委托代理证书 (K,V) 是安全的，因此攻击者A不能伪造一个新的授权证书。② 代理签名的存在性不可伪造性。

定理6 在DLP困难性假设下，最终代理签名 (N,B',S) 不可伪造。

证明 若A直接构造 B' 通过式(6)来伪造 S，需求解离散对数，或先伪造部分签名 S'_i，但经下述证明 S'_i 不可伪造：若A直接随机选择 n_i 和 c_i，由 $S'_i=(T_i c_i+n_i N)\cdot(B+\bar{M}h(W)) \bmod q$ 计算 S'_i，使其通过式(4)是困难的；而在DLP困难性假设下，通过 $N_i=g^{n_i} \bmod p$ 和 $C_i=g^{c_i} \bmod p$ 求解 n_i 和 c_i 是困难的。

综上所述，本方案满足不可伪造性。

(3)不可否认性

① 原始签名组不能否认对代理签名组的授权。委托代理证书 (K,V) 满足验证式(5)，而(5)式中涉及到所有原始签名人的私钥信息，故原始签名组不能否认其授权。

② 代理签名组不能否认对消息 M 的签名。在2.3节代理签名密钥生成阶段，P_j 只有利用自己的私钥才能构造满足 $a_{j0}=(x_{P_j}+n_j V) \bmod q$ 的多项式 $f_j(x)$，且验证

式(3)中涉及到 P_j 的公钥 y_{P_j};再验证最终签名的有效性,即式(6)也用到所有 P_j 的公钥之积 Y 。因此代理签名组不能否认其代理签名。

(4)可追踪性

当发生纠纷时,可根据最终签名 (N,B',S) 中 N 的唯一性查出实际参与签名的 t 个代理签名人的身份,即本方案对实际参与签名人的身份有可追踪性。

(5)鲁棒性

与文献[5,13-15]中方案相比,本文方案在代理签名生成阶段加入了一个门限代理过程,只要 t 个(并不需要全部)代理签名人便可完成签名。故当有个别代理签名人因特殊情况不能参与签名,不会影响本方案执行,即本方案具有良好的鲁棒性和容错性。

(6)盲性

本方案在代理签名生成阶段不同于文献[5,13-15],U_l 先用随机数 α、β 将 M 盲化为 $\bar{M}$,然后将 B 和 $\bar{M}$ 发送给 E 中成员 P_i ,而 P_i 想要通过式 $\bar{M}=(\alpha^{-1}h(M\|B')+\beta)\bmod q$ 获取消息 M 是不可能的。因此 E 中每个 P_i 都无法获取自己所签署消息的具体内容,即本方案具备盲性。

(7)不可链接性

当 U_l 公布一个 M 的最终签名 (N,B',S) ,即使 E 中所有 P_i 保留每一次签名的中间变量 B_i 并联合起来求出 B ,且通过 $B'=(\alpha B+\alpha\beta h(W))\bmod q\,\bar{M}=\alpha^{-1}h(M\|B')+\beta\bmod q$ 求出盲化因子 α 和 β 。但因 α 和 β 是随机选择的,P_i 仍不知此签名 (N,B',S) 是对应哪次中间变量 B_i ,即 P_i 不能将最终签名与签名过程所用具体消息联系起来,它们是相互独立的,因此方案满足不可链接性,有效保护消息拥有者的隐私。

(8)防止签名权利的滥用

W 中明确规定了代理签名的消息范围及代理有效期限,可防止代理签名人滥用自己的代理权。因为代理私钥中含有原始签名人和代理签名人的私钥,只能用于代理签名,这样可以确保代理私钥不能用于除产生有效代理签名以外的其他目的。

3.3 性能分析

(1)定性分析结果

方案的特性比较见表1。

表1 方案特性比较

方案特性	本文方案	文献[5,13-15]方案
门限签名性	有	无
盲签名性	有	无
多重代理多重签名性	有	有
安全性	强	弱

(2)定量分析结果

① 与文献[5,13-15]中的方案比较,本文方案在代理证书生成阶段,将 $V_{U_i}=h(W)x_{U_i}y_{U_i}+k_{U_i}K\bmod q$ 改为 $V_{U_i}=h(W)x_{U_i}+k_{U_i}K\bmod q$,验证式(1)相应改为 $g^{V_{U_i}}=y_{U_i}^{h(W)}L_{U_i}{}^{K}\bmod p$,同样 V_{P_j} 也做了相应的改进;最后验证式(5)相应改为 $g^{V}=K^{K}(\prod_{i=1}^{m}y_{U_i}\prod_{j=1}^{n}y_{P_j})^{h(W)}\bmod p$,这样不仅大大减少了运算复杂度,且方案安全特性不受影响。

② 本文方案2.3~2.5节共进行了 $(3n^2-2n+(n+4)t+7)T_{\exp}+(n^2-n+2t+5)\,T_{\mathrm{mul}}$,其中 $T_{\exp}$ 为一次模幂运算时间,T_{mul} 一次模乘运算时间。与文献[5,13-15]中的方案相比,本方案为实现鲁棒性、盲性和不可链接性而导致计算量略有增加。

4 结束语

指出文献[5,13-15]方案中存在的安全缺陷,用门限思想避免了因某个代理签名人缺席或出错导致签名无法进行的缺陷,增强了方案的鲁棒性与容错性,同时用盲化消息的思想使得代理签名人对敏感的签名消息不知情,设计了一个高效的门限多重代理多重盲签名方案。经过安全性分析表明,本文方案比一般的多重代理多重签名方案具有更强的灵活性和容错性,具有广泛的应用场景。

参考文献:

[1] Mambo M, Usuda K, Okamoto E.Proxy signatures for delegating signing operation[C]//Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, 1996:48-57.

[2] Shao Z.Improvement of identity-based proxy multi-signature scheme[J].The Journal of Systems and Software, 2009,82(5):794-800.

[3] 姜东焕,徐光宝.安全的有代理的多重签名方案[J].计算机工程与应用,2010,46(33):115-116.

[4] Liu Zhenhua, Hu Yupu, Zhang Xiangsong et al.Provably secure multi-proxy signature scheme with revocation in the standard model[J].Computer Communications, 2011, 34(3):494-501.

[5] 李传目.多重代理多重签名方案[J].计算机工程,2003,29(21):43-44.

[6] Kim S, Park S, Won D.Proxy signatures, revisited[C]//Proceedings of the 1st International Conference on Information and Communications Security.Berlin:Springer-Verlag, 1997:223-232.

[7] Zhang K.Threshold proxy signatures schemes[M]//Okamoto E, Davida G, Mambo M.Proceedings of the Information Security.Berlin:Springer-Verlag, 1998:191-197.

(下转146页)

5 结束语

为了提高基于外辐射源的单站无源目标跟踪精度，提出了一种带二次约束的容积卡尔曼跟踪算法。将二次约束作为观测方程引入容积卡尔曼滤波，并通过仿真实验测试算法性能。仿真结果表明，目标在不同二次约束运动模型下，相对于传统的投影无迹卡尔曼滤波算法和无迹卡尔曼滤波算法，本文算法稳定性更强，具有更高的目标跟踪精度。

参考文献：

[1] Shen J，Mo8lisch A F，Salmi J.Accurate passive location estimation using TOA measurements[J].IEEE Transactions on Wireless Communications，2012，11(6)：2182-2192.

[2] Berger C R，Demissie B，Heckenbach J，et al.Signal processing for passive radar using OFDM waveforms[J].IEEE Journal of Selected Topics in Signal Processing，2010，4(1)：226-238.

[3] Wang H，Wang J，Zhong L.Mismatched filter for analogue TV-based passive bistatic radar[J].IET Radar，Sonar & Navigation，2011，5(5)：573-581.

[4] 霍光，李冬海，李晶.基于强跟踪容积卡尔曼滤波的单站无源跟踪算法[J].现代雷达，2013，35(11)：52-57.

[5] Simon D.Kalman filtering with state constraints：A survey of linear and nonlinear algorithms[J].IET Control Theory & Applications，2010，4(8)：1303-1318.

[6] Teixeira B O S，Chandrasekar J，Tôrres L A B，et al.State estimation for linear and non-linear equality-constrained systems[J].International Journal of Control，2009，82(5)：918-936.

[7] Yang C，Blasch E.Kalman filtering with nonlinear state constraints[J].IEEE Transactions on Aerospace and Electronic Systems，2009，45(1)：70-84.

[8] Arasaratnam I，Haykin S.Cubature Kalman filters[J].IEEE Transactions on Automatic Control，2009，54(6)：1254-1269.

[9] Yousefi S，Chang X W，Champagne B.Mobile localization in non-line-of-sight using constrained square-root unscented Kalman filter[J].IEEE Transactions on Vehicular Technology，2015，64(5)：2071-2083.

[10] Jia B，Xin M，Cheng Y.High-degree cubature Kalman filter[J].Automatica，2013，49(2)：510-518.

[11] Leong P H，Arulampalam S，Lamahewa T A，et al.A Gaussian-sum based cubature Kalman filter for bearings-only tracking[J].IEEE Transactions on Aerospace and Electronic Systems，2013，49(2)：1161-1176.

[12] Chang L，Hu B，Li A，et al.Transformed unscented Kalman filter[J].IEEE Transactions on Automatic Control，2013，58(1)：252-257.

[13] 孙枫，唐李军.Cubature卡尔曼滤波与Unscented卡尔曼滤波估计精度比较[J].控制与决策，2013，28(2)：303-308.

[14] Zarei J，Shokri E.Nonlinear and constrained state estimation based on the cubature Kalman filter[J].Industrial & Engineering Chemistry Research，2014，53(10)：3938-3949.

[15] 戴定成，蔡宗平，牛创.基于简化平方根容积卡尔曼滤波的跟踪算法[J].电光与控制，2015，22(3)：11-14.

[16] 单甘霖，张凯，吉兵.基于高斯和均方根容积卡尔曼滤波的姿态角辅助目标跟踪算法[J].电子与信息学报，2014，36(7)：1579-1584.

[17] Leong P H，Arulampalam S，Lamahewa T，et al.Gaussian-sum cubature Kalman filter with improved robustness for bearings-only tracking[J].IEEE Signal Processing Letters，2014，21(5)：513-517.

[18] Teixeira B O S，Chandrasekar J，Tôrres L A B，et al.Unscented filtering for equality-constrained non-linear systems[C]//Proceedings of American Control Conference，2008：39-44.

（上接133页）

[8] Sun H M.An efficient nonrepudiable threshold proxy signature scheme with known signers[J].Computer Communications，1999，22(8)：717-722.

[9] 李继国，曹珍富，李建中，等.代理签名的现状与发展[J].通信学报，2003，24(10)：114-124.

[10] 于义科，郑雪峰.标准模型下基于身份的高效动态门限代理签名方案[J].通信学报，2011，32(8)：55-63.

[11] 徐太平，陈勇.抗合谋攻击的门限混合代理多重签名方案[J].计算机工程与应用，2013，49(14)：73-76.

[12] Chaum D.Blind signatures for untraceable payments[C]//Advances in Crypto'82，Plenum，NY，1982：199-203.

[13] 门玉梅，王勇兵，张建中.多重代理多重签名方案的分析与改进[J].河南师范大学学报：自然科学版，2009，37(1)：27-30.

[14] 丁薇，张建中.一种新的多重代理多重数字签名方案[J].计算机应用研究，2010，27(8)：3081-3082.

[15] 张兴华.一个新的基于离散对数问题的多重代理多重签名方案[J].计算机应用与软件，2014，31(2)：317-320.

[16] 张文芳，何大可，王宏霞，等.具有可追查性的抗合谋攻击(t,n)门限签名方案[J].西南交通大学学报，2007，42(4)：461-467.

[17] Gu C，Zhu Y.Provable security of ID-based proxy signature schemes[C]//Proceedings of ICCNMC'05.Berlin：Springer-Verlag，2005：1277-1286.

[18] 黄茹芬，农强，黄振杰.可证安全的基于证书部分盲签名方案[J].计算机工程，2014，40(6)：109-114.