一种基于双线性对的公开可验证多秘密共享方案

张柄虹[1]， 张串绒[1]， 焦和平[2]， 张欣威[1]， 高胜国[3]
(1.空军工程大学信息与导航学院,陕西西安,710077;2.西北工业大学,陕西西安,710072;
3.77100部队,重庆,400014)

摘要 针对部分多秘密共享方案的安全性依赖于单一系数的问题,基于双线性对和Shamir门限体制,设计了一种可公开验证的多秘密共享方案。在该方案中,参与者的私钥计算和秘密分发过程分离,参与者私钥由参与者自己选择且只需保存一个私钥,就可以实现共享任意多个秘密。在秘密分发阶段和秘密恢复阶段具有可公开验证性,任何人都可以验证秘密份额的正确性,有效防止了不诚实参与者和分发者的欺诈行为。秘密分发者与参与者在公开信道中传输信息而不需要维护一个秘密信道,降低了系统开销。多秘密的共享分布在多个系数当中,单个系数或秘密的泄漏不会造成其他秘密的泄露,同时椭圆曲线离散对数和双线性Diffie-Hellman问题的求解困难性,确保了方案的安全性。最后对方案的正确性和拓展性等给出了数学证明和理论分析。

关键词 多秘密共享;双线性对;门限密码;可验证方案
DOI 10.3969/j.issn.1009-3516.2014.04.020
中图分类号 TN918.1 **文献标志码** A **文章编号** 1009-3516(2014)04-0083-05

A Public Verifiable Multi-secret Sharing Scheme Based on Bilinear Pairings

ZHANG Bing-hong[1],ZHANG Chuan-rong[1],JIAO He-ping[2],ZHANG Xin-wei[1],GAO Sheng-guo[3]
(1. Information and Navigation College, Air Force Engineering University, Xi'an 710077, China;
2.Northwestern Polytechnical University,Xi'an 710072, China;
3.Unit 77100, Chongqing 400014, China)

Abstract: Aimed at the problem that the security of some multi-secret sharing schemes only depends on a single coefficient, and based on the bilinear pairings and the Shamir threshold scheme, this paper proposes a public verifiable secret scheme. In the scheme, the secret key computation of participant is apart from the process of secret distribution. The secret key is chosen by the participant himself and the participant only needs to keep one secret key. By so doing the multi- secrets sharing at will in the process can be realized. The public verifiable scheme is effectively applied in the process of the secret distribution and the secret recovery ,so that anyone could be able to verify the correctness of the share to effectively prevent the dishonest participant and the dealer from cheating. The dealer and the participant transmit information through the public channel rather than the secret channel, thus reducing the system costs. The sharing of multi-se-

收稿日期:2013-12-31
基金项目:国家自然科学基金资助项目(61272486)
作者简介:张柄虹(1989—),男,四川江油人,硕士生,主要从事密码学与信息安全,密钥管理研究.E-mail:zbh_1989ing@163.com

引用格式:张柄虹,张串绒,焦和平,等. 一种基于双线性对的公开可验证多秘密共享方案[J]. 空军工程大学学报:自然科学版,2014,15(4):83-87. ZHANG Binghong,ZHANG Chuanrong,JIAO He-ping,et al.A Public Verifiable Multi-secret Sharing Scheme Based on Bilinear Pairings [J].Journal of air force engineering university:natural science edition,2014,15(4):83-87.

cret lies in multiple coefficients, and the leak of a single coefficient or secret does not lead to the leak of other secrets. By using the Elliptic Curve Discrete Logarithm Problem and Bilinear Diffie-Hellman Problem, the security of the scheme is guaranteed. At last, mathematical proof and theoretical analysis of validity and expansion of the scheme are given.

Key words: multi-secret sharing; bilinear pairings; threshold cryptography; verifiable scheme

秘密共享是密码学中十分重要的研究内容,在信息安全和数据保密中具有十分重要的作用。自秘密共享的概念由 Shamir[1] 和 Blakley[2] 分别根据 Lagrange 差值多项式和矢量空间的性质提出以来,人们围绕秘密共享进行了深入的研究。Shamir 与 Blakley 提出的方案都是基于所有参与者都是诚实的这一前提,不能解决不诚实的秘密分发者和参与者欺诈的问题。同时一个秘密共享过程只能分享一个秘密。Stadler[3] 提出的公开可验证的秘密共享方案,任何人都可以通过公开量对秘密份额的正确性进行验证。同时,在公开可验证的秘密共享方案中,秘密分发者广播信息给参与者而不需要维护一个秘密信道,降低了系统的开销。文献[4]基于门限思想与椭圆曲线离散对数提出了一种一般结构中的多秘密共享算法,不需要安全通道,实现动态验证。

基于椭圆曲线的方案能够在保证同等安全性的前提下,大大减少系统的计算开销,提高效率。李慧贤等[5]基于椭圆曲线上的双线性变换提出的可证明安全的秘密共享方案将参与者私钥计算和秘密分发过程分离,具有很好的安全性和效率。文献[6~7]基于双线性对分别提出可公开验证秘密共享方案,秘密分发者广播秘密份额的信息,参与者利用自己的私钥解密,确保了秘密份额的安全性,并利用公开量进行验证,降低了系统存储量和计算量,但一个共享过程只能共享一个秘密。黄伟达等[8]基于双线性对提出动态门限多秘密共享方案,利用双线性对进行验证,无需安全通道,但方案的安全性依赖于单一多项式系数 a_0,知道一个秘密,即可利用公开信息,通过简单运算得到其他秘密。

本文基于文献[4]中的多秘密共享思想,提出一种基于双线性对的可公开验证的多秘密共享方案,该方案消除了文献[8]所提出方案只依赖于单一系数的弊端,将秘密安全性分布在不同的系数中,其中某个秘密泄露,不会影响其他秘密的安全性。参与者只需维护一个私钥,就可以在每个共享过程共享任意多个秘密。基于公开可验证的思想,对秘密分发和秘密恢复过程进行公开验证,有效解决不诚实秘密分发者和参与者的欺诈问题。

1 基础知识

椭圆曲线公钥密码[9]作为一种新型的快速公钥密码算法,凭借其安全性高、计算量小、带宽要求低的特点成为公钥密码算法的研究热点。

1.1 椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem,ECDLP)

用 $E(GF(p^m))$ 表示定义于有限子域 $GF(p)$ 上的椭圆曲线在 m 次扩域上的有理子群,P,Q 为 $E(GF(p^m))$ 上的任意 2 点,已知某整数 k,有 $Q=kP$。则由 P,Q 和 $E(GF(p^m))$ 求出 k 是困难的。

1.2 双线性对(Bilinear Pairing)映射

令 G 是阶为 q 的循环加法群,q 是一个大素数,P 是 G 的生成元,G_1 为具有相同阶 q 的循环乘法群,a,b 为 Z_q^* 中的元素。映射 $e:G\times G\to G_1$ 称为双线性映射,并且拥有以下性质:

1)双线性:$\forall P,Q\in G,\forall a,b\in Z_q^*$,$e(aP,bQ)=e(P,Q)^{ab}$;

2)非退化性:存在 $P,Q\in G$,使得 $e(P,Q)\neq 1$。

3)可计算性:对于所有 $P,Q\in G$,总存在有效的计算方法计算 $e(P,Q)$。

1.3 计算性 Diffie-Hellman 问题

给定(P,aP,bP),计算 $abP\in G$,其中 $a,b\in Z_q^*$ 是未知的整数。

1.4 双线性 Diffie-Hellman 问题

给定(P,aP,bP,cP),计算 $e(P,P)^{abc}\in G_1$,这里 $a,b,c\in Z_q^*$ 是未知的整数。

一般认为任何算法在多项式时间内解决计算性 Diffie-Hellman 问题、双线性 Diffie-Hellman 问题时,不具有优势。

2 基于双线性对的多秘密共享方案

基于双线性对快速高效,存储量小的优点,利用公开可验证的方法,提出一种多秘密共享方案。方案分为 4 个阶段:初始化阶段、秘密分发阶段、验证阶段和秘密恢复阶段。

2.1 系统初始化

方案需要一个公告板,用于存放一些公开量,只有秘密分发者 Dealer(下文简记为 D)可以修改公告

板上的信息,其他参与者只能阅读。秘密分发者负责系统公钥的计算和发布,并将参与者公钥和与秘密相关的信息公布在公告板上。

记 $U=\{U_1,U_2,\ldots,U_n\}$ 为 n 个秘密参与者的集合,秘密分发者 D 随机选择一个 $s\in Z_q^*$ 作为系统私钥,计算 $P_{pub}=sP$ 作为系统公钥。秘密分发者 D 随机选择一组秘密参数 $a_1,a_2,\ldots,a_p\in Z_q^*$,计算秘密 $s_1=a_1P_{pub},s_2=a_2P_{pub},\ldots,s_p=a_pP_{pub}$,并将秘密分发给参与者。

每个秘密参与者 U_i 随机选择自己的私钥 $d_i\in Z_q^*$,将 $P_i=d_iP_{pub}$ 作为自己的公钥发送给 D,并由 D 确定 $P_i\neq P_j,i\neq j$。若 $P_i=P_j,i\neq j$,则要求参与者重新选择 $d_i\in F_q^*,i=1,2,\ldots n$,直到 $P_i\neq P_j,i\neq j$。D 将 P,P_{pub},P_i 公布在公告板上。

2.2　秘密分发阶段

1)当 $p\leqslant t$ 时,秘密分发者 D 构造一个 $t-1$ 次的多项式:

$$f(x)=\sum_{i=1}^{p}a_ix^{i-1}+\sum_{j=1}^{t-p}b_jx^{j-1+p}=\sum_{i=1}^{t}z_ix^{i-1}\tag{1}$$

式中 $b_j\in Z_q^*$,$z_i=\begin{cases}a_i,i=1,2,\ldots,p\\b_{i-p-1},i=p,\ldots,t-1\end{cases}$。

秘密分发者 D 随机选择 $r_i\in Z_q^*$,计算以下值:$Z_j=z_jP,X_i=f(i)P,Y_i=f(i)P_i,\alpha_i=r_iP,\beta_i=r_iP_i,\gamma_i=(r_i+f(i))P_{pub}$,其中 $i=1,2,\ldots,n;j=1,2,\ldots,t$,并公布所有的 $Z_j,Y_i,\alpha_i,\beta_i,\gamma_i$,其中 X_i 可以由 Z_j 计算:

$$X_i=f(i)P=\sum_{j=1}^{t}z_ji^{j-1}P=$$

$$\sum_{j=1}^{t}(i^{j-1})z_jP=\sum_{j=1}^{t}(i^{j-1})Z_j\tag{2}$$

2)当 $p>t$ 时,秘密分发者 D 构造一个 $p-1$ 次的多项式:

$$f(x)=\sum_{i=1}^{p}z_ix^{p-1}\tag{3}$$

式中:$z_i=a_i,i=1,2,\ldots,p$,并随机选择 $r_i\in Z_q^*$,计算以下列值:$Z_j=z_jP,X_i=f(i)P,Y_i=f(i)P_i,\alpha_i=r_iP,\beta_i=r_iP_i,\gamma_i=(r_i+f(i))P_{pub}$,其中 $i=1,2,\ldots,n,j=1,2,\ldots,p$。

公开所有的 $Z_j,Y_i,\alpha_i,\beta_i,\gamma_i$,其中 X_i 可以由 Z_j 计算:

$$X_i=f(i)P=\sum_{j=1}^{p}z_ji^{j-1}P=$$

$$\sum_{j=1}^{p}(i^{j-1})z_jP=\sum_{j=1}^{p}(i^{j-1})Z_j\tag{4}$$

计算并公布 $S_i'=f(i)P_{pub},i=n+1,n+2,\ldots,n+p-t$。

2.3　对秘密分发者的验证

参与者首先计算 $X_i=\sum_{j=1}^{p}(i^{j-1})Z_j$,并根据公开量验证下列等式是否成立:

$$\begin{cases}e(P,\sum_{i=1}^{n}\gamma_i)=e(P_{pub},\sum_{i=1}^{n}(\alpha_i+X_i))\\\prod_{i=1}^{n}e(P_i,\gamma_i)=e(P_{pub},\sum_{i=1}^{n}(\beta_i+Y_i))\end{cases}\tag{5}$$

若验证不通过,表明秘密分发者存在欺骗行为,参与者退出秘密共享过程;若以上验证通过,则表明秘密分发者没有欺骗行为,可以信任,秘密分发过程继续。

秘密参与者 P_i 利用自己的私钥 d_i 及公开量计算对应的秘密份额 $S_i=d_i^{-1}Y_i=d_i^{-1}f(i)d_iP_{pub}=f(i)P_{pub}$,秘密分发过程结束后,分发者 D 退出。

2.4　秘密恢复阶段

在秘密恢复阶段,至少 t 个秘密参与者 U_i(这里我们假设为 $U_1,U_2,\ldots,U_t$)贡献自己的秘密份额 $S_i(i=1,2,\ldots,t)$。

秘密恢复者首先验证等式是否成立:

$$e(\beta_iP_{pub},P)e(S_iP_i,P)=e(\gamma_i,PP_i)\tag{6}$$

如果等式不成立,则表明参与者 U_i 存在欺骗行为;如果等式成立,则表明参与者 U_i 没有欺骗行为,贡献了正确的秘密份额。

1)当 $p\leqslant t$ 时,根据拉格朗日差值,秘密恢复者依靠参与者提供的 t 个秘密份额,可以得到:

$$\sum_{i=1}^{t}S_i\lambda_i=f(x)P_{pub}=$$

$$(\sum_{i=1}^{p}a_ix^{i-1}+\sum_{j=1}^{t-p}b_jx^{j-1+p})P_{pub}\tag{7}$$

式中 $\lambda_i=\prod_{j=1,i\neq j}^{t}\frac{x-j}{i-j}$。

2)当 $p>t$ 时,秘密恢复者依靠参与者提供的 t 个秘密份额,并从公告板下载 $p-t$ 个公开量 $S_i'=f(i)P_{pub},(i=n+1,n+2,\ldots,n+p-t)$,可得:

$$\sum_{i=1}^{p}S_i\lambda_i=f(x)P_{pub}=\sum_{i=1}^{p}z_ix^{p-1}P_{pub}\tag{8}$$

式中 $\lambda_i=\prod_{j=1,i\neq j}^{p}\frac{x-j}{i-j}$。

由上述过程可以得到分享的 p 个秘密 $s_1=a_1P_{pub},s_2=a_2P_{pub},\ldots,s_p=a_pP_{pub}$。

3　分析与讨论

3.1　正确性分析

1)在秘密共享过程中,分发者 D 在公告板上公

布了一系列的参数,为了防止秘密分发者的欺诈行为,需要对秘密分发者公布的参数进行验证。式(5)验证过程的证明如下:

证明 $e(P,\sum_{i=1}^{n}\gamma_i)=e(P,\sum_{i=1}^{n}(r_i+f(i))P_{pub})=e(P_{pub},\sum_{i=1}^{n}(r_i+f(i))P)=e(P_{pub},\sum_{i=1}^{n}(\alpha_iP+X_iP))=e(P_{pub},\sum_{i=1}^{n}(\alpha_i+X_i));\prod_{i=1}^{n}e(P_i,\gamma_i)=\prod_{i=1}^{n}e(P_i,(r_i+f(i))P_{pub})=\prod_{i=1}^{n}e(P_{pub},(r_i+f(i))P_i)=e(P_{pub},\sum_{i=1}^{n}(\beta_i+Y_i))$

2) 在秘密恢复阶段,秘密参与者可能提供伪造的秘密份额,使得其他参与者不能恢复出正确的秘密,因而需要对参与者提供的秘密份额进行。式(6)验证过程的证明如下:

证明 $e(\beta_iP_{pub},P)e(S_iP_i,P)=e(\beta_iP_{pub}+S_iP_i,P)=e(r_iP_iP_{pub}+f(i)P_{pub}P_i,P)=e((r_i+f(i))P_{pub},PP_i)=e(\gamma_i,PP_i)$

通过对秘密分发者和秘密参与者的公开验证,可以确保秘密正确的分发以及恢复,有效防止欺诈行为的发生。

3.2 安全性分析

对方案的攻击主要有参与者的合谋窃取秘密,攻击者根据公开信息计算得到秘密以及攻击者伪造身份和秘密份额,进而获取秘密等几种类型。下面根据这几种攻击类型对方案的安全性进行分析。

1)$t-1$ 个或者更少的参与者企图恢复秘密。因为本文基于 Shamir 的门限体制的,在 $t-1$ 次多项式中只有不少于 t 个数值对$(i,f(i))$才能恢复多项式 $f(x)$。所以秘密恢复阶段,少于 t 个参与者无法恢复秘密。只有不少于 t 个参与者正确无欺诈地贡献出自己的秘密份额之后,利用拉格朗日差值多项式才能恢复秘密。

2)攻击者根据公告板上的信息获取秘密。攻击者要根据公告板上信息 $P_{pub}=sP$,$P_i=d_iP_{pub}$,$s_i=a_iP_{pub}$来计算得到秘密分发者和参与者私钥 s,d_i 以及秘密参数 a_i。这是椭圆曲线上的离散对数难题,要想计算得到 d_i,s,a_i 是不可能的。

3)攻击者伪造秘密份额 S_k。秘密恢复者利用 $e(\beta_iP_{pub},P)e(S_iP_i,P)=e(\gamma_i,PP_i)$对秘密份额进行验证,因为攻击者不可能从公告板得出有关多项式的任何参数信息,因而伪造的秘密份额 S_k 不可能通过验证。

3.3 性能分析

1)本方案是基于椭圆曲线上的双线性对提出的,较基于RSA 体制的秘密共享方案[10-11]具有通信成本低和存储空间小的特点。椭圆曲线上的离散对数问题,能够使本文提出的方案在同等安全性的条件下使用短密钥。分发者和参与者只需要保存自己的私钥,其他信息均在公告板上公开,存储量少。

2)参与者的秘密份额由参与者自己选择和保管,并计算公钥,秘密分发者并不知道参与者的私钥,减少了秘密分发者的计算量。所有信息均在公开信道上传输,不需要维护秘密信道,降低了系统的开销。参与者根据公告板上的信息对秘密分发者公布的信息进行验证,并用自己的私钥计算出自己的秘密份额。

3)与文献[6]提出的方案相比,本文在秘密参与者不改变自己私钥的条件下实现了任意个秘密的共享,提高了方案的效率。同时在秘密恢复阶段,增加了秘密恢复者对秘密份额的验证,有效避免了秘密恢复阶段参与者以及第 3 方攻击者的欺诈行为。

4)与文献[8]提出的方案相比,安全性提高,多秘密的安全性不依赖于单一系数 a_0,而是将秘密的安全性分布在各个系数中。即使单个秘密 s_k 泄露,攻击者也不可能根据公开信息得到其他秘密信息。

5)从方案的扩展性来看,若有新成员 U_k 加入,则只需要自己选择私钥 d_k,并计算公钥 $P_k=d_kP_{pub}$,$(P_k\neq P_i,i=1,2,\ldots,n)$,秘密分发者 D 计算对应的公开量,其他参与者不需要任何变化。若有成员 U_k 退出,则只需要秘密分发者 D 在公告板上删除 U_k 所对应的公开信息即可。

4 结语

本文基于双线性对提出了一种公开可验证的多秘密共享方案,每个参与者私钥由参与者自己选择,秘密分发者不知道各参与者的私钥,且参与者只需维护自己的私钥就可以实现任意多个秘密的共享,提高方案的效率。利用公开信息进行验证,避免了秘密分发者和参与者的欺诈。所有信息都在公开信道上传输,不需要维护秘密信道,降低了系统的运行开销。多秘密的安全性分布于多个系数中,而不依赖单一系数,提高了方案的安全性。

参考文献(References):

[1] Shamir A. How to share a secret[J].Communications of the ACM, 1979, 22(11): 612-613.

[2] Blakey G R.Safeguarding cryptographic keys[C]//IEEE computer society.Los Alamitos, CA: IEEE press, 1979: 313-317.

[3] Stadler M.Public verifiable secret sharing[J].EUROCRYPT,LNCS,1996,1070: 190-199.

[4] YE Saizhi, YAO Guoxiang, GUAN Quanlong. A multiple secret sharing scheme with general access structure[C]//2009 international symposium on intelligent ubiquitous computing and education. Chengdu: IEEE computer science, 2009: 461-464.

[5] 李慧贤,庞辽军.基于双线性变换的可证明安全的秘密共享方案[J].通信学报,2008,29(10):45-50.
LI Huixian, PANG Liaojun. Provably secure secret sharing scheme based on bilinear maps[J]. Journal on communications, 2008, 29(10): 45-50.(in Chinese)

[6] Wu TsuYang, Tseng Yuh-Min. A pairing-based publicly verifiable secret sharing scheme[J]. Journal of systems science and complexity, 2011, 24(1): 186-194.

[7] Somayeh Heidarvand, Jorge L Villar. Public verifiability from pairings in secret sharing schemes[J]. Lecture notes in computer science, 2009, 5381(1): 294-308.

[8] 黄伟达,姚国祥,沈瑞雪.基于双线性对的动态门限多秘密共享方案[J].计算机工程与设计,2012,33(3):901-905.
HUANG Weida, YAO Guoxiang, SHEN Ruixue. Dynamic threshold multi-secret sharing scheme based on bilinear pairing[J]. Computer engineering and design, 2012, 33(3): 901-905.(in Chinese)

[9] Koblitz N. Elliptic curve cryptosystems[J]. Mathematics of computation, 1987, 48: 203-209.

[10] 庞辽军,王育民.基于 RSA 密码体制(t, n)门限秘密共享方案[J].通信学报, 2005, 26(6): 70-73.
PANG Liaojun, WANG Yumin. (t, n) threshold secret sharing scheme based on RSA crypto system[J]. Journal of China institute of communications, 2005, 26(6): 70-73.(in Chinese)

[11] 黄东平,刘铎,王道顺,等.一种安全的门限多秘密共享方案[J].电子学报,2006,34(11):1937-1940.
HUANG Dongping, LIU Duo, WANG Daoshun, et al. A secure threshold multi-secret sharing scheme[J]. Acta electronica sinica, 2006, 34(11): 1937-1940.(in Chinese)

(编辑:徐楠楠)

(上接第 78 页)

[2] LIU Zhong, HE Jingbo. Passive location algorithm using kushner equation[J]. Journal of theoretical and applied information technology, 2013, 47(7): 229-232.

[3] 吴昊, 陈树新, 侯志强,等. 一种鲁棒的约束总体最小二乘定位算法[J]. 上海交通大学学报:自然科学版,2013,47(7):1114-1118.
WU Hao, CHEN Shuxin, HOU Zhiqiang, et al. A robust constrained total least squares algorithm for passive location[J]. Journal of Shanghai jiaotong university: natural science edition, 2013, 47(7): 1114-1118.(in Chinese)

[4] ZHOU Y, LI J X. Collaborative maneuvering target tracking in wireless senor network with quantized range-only measurements[J]. IEEE signal processing letters, 2009, 17(2): 157-160.

[5] 杨元喜.自适应动态导航定位[M].北京:测绘出版社, 2006.
YANG Yuanxi. Adaptive navigation and kinematic positioning[M]. Beijing: Surveying and mapping publishing house, 2006.(in Chinese)

[6] HUANG G, ZHANG Q. Real-time estimation of satellite clock offset using sdaptively robust Kalman filter with classified adaptive factors[J]. GPS solution, 2012, 16(4): 531-539.

[7] 聂建亮, 张双成. 基于抗差 Kalman 滤波的精密单点定位[J]. 地球科学与环境学报, 2010, 32(6): 218-220.
NIE Jianliang, ZHANG Shuangcheng. Precise point positioning based on robust Kalman filtering[J]. Journal of earth sciences and environment, 2010, 32(6): 218-220.(in Chinese)

[8] 王坚, 刘超, 高井祥,等. 基于抗差 EKF 的 GNSS/INS 紧组合算法研究[J].武汉大学学报, 2011, 36(5): 596-600.
WANG Jian, LIU Chao, GAO Jingxiang, et al. GNSS/INS tightly coupled navigation model based on robust EKF[J]. Geomatics and information science of Wuhan university, 2011, 36(5): 596-600.(in Chinese)

[9] YANG Ji. The EKF senorless control strategy of permanent magnet synchronous motor adaptive back stepping control system[C]//Applied mechanics and mechanical engineering III. Wuhan: [s.n.] 2013: 1166-1172.

[10] Bhatti U I, Ochieng W Y, FENG Shaojun. Integrity of an integrated GPS/INS system in the presence of slowly growing errors. part I: a critical review [J]. GPS sloution, 2007, 11(3): 173-181.

[11] 周彦,李建勋,王冬丽.传感器网络中鲁棒状态信息融合抗差卡尔曼滤波器[J].控制理论与应用, 2012, 29(3): 291-297.
ZHOU Yan, LI Jianxun, WANG Dongli. Anti-outlier Kalman filter-based robust estimation fusion in wireless sensor networks[J]. Control theory & applications, 2012, 29(3): 291-297.(in Chinese)

(编辑:徐楠楠)