一种抗不诚实第三方攻击的一次性公钥方案

柴林鹏 张 斌

(信息工程大学 郑州 450001) (河南省信息安全重点实验室 郑州 450001)

摘 要 针对现有典型一次性公钥方案无法抵抗不诚实第三方恶意攻击的问题,提出一种可对第三方行为进行双重约束的一次性公钥改进方案。基于该方案,用户和服务提供方可通过第三方发布的身份索引及私钥生成过程中的公开可验证消息对其诚实性进行判断,从而约束第三方的不诚实行为。同时,采用的索引生成算法在一定程度上提高了对恶意用户的追踪效率。

关键词 匿名性,基于身份密码体制,一次性公钥,公开可验证

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.07.023

One-off Public Key Scheme for Preventing Dishonest Third Party Attacking

CHAI Lin-peng ZHANG Bin

(Information Engineering University, Zhengzhou 450001, China)

(Henan Province Information Security Key Laboratory, Zhengzhou 450001, China)

Abstract Aiming at the problem that the existing schemes cannot resist the malicious behaviors of the dishonest third party, this paper proposed an improved one-off public key scheme that can doubly restrain the behaviors of the third party. In this scheme, users and service providers can judge whether the third party is honest or not via verifying the identity index published by the third party and the publicly verifiable information generated during the private key extraction, and this scheme can restrain the dishonest behaviors of the third party consequently. At the same time, the index algorithm can improve the efficiency of trace for malicious users.

Keywords Anonymity, Identity-based cryptography, One-off public key, Public verifiability

1 引言

身份认证机制作为保证互联网中商务活动安全的第一道“屏障”,可以确定通信双方的真实身份,但认证过程需要通信双方提供真实的身份信息,这为恶意攻击者跟踪用户网络行为提供了便利,因此用户面临着真实身份等隐私信息泄露的安全风险。为了保护用户的隐私,身份认证方案在满足安全性的同时,也需要满足以下安全属性[1]:1)强匿名性,在认证过程中,通信方和外部用户只能确定用户身份的合法性,但是无法分析出与用户真实身份相关的任何信息;2)不可伪造性,合法用户和攻击者均无法对合法签名进行伪造;3)可追踪性,第三方能够依据服务提供方提供的认证信息揭示出恶意用户的真实身份。

针对上述要求,目前已提出多种认证技术,其中一类是假名技术[2-3],然而该类技术需要提前向第三方申请多个假名证书或者多次向第三方申请假名,且要求服务器管理所有用户的全部证书,证书管理开销大,对用户端的存储能力要求高或者要求第三方实时参与用户假名分发。一旦第三方被攻破或者发起恶意攻击,用户将面临隐私泄露的安全风险。另一类是一次性公钥技术[1,4-8],该技术的核心思想是第三方只需为用户颁发一次用户私钥,然后由用户结合随机数生成可用于验证身份合法性的一次性公钥,可有效解决匿名通信问题。张秋璞等于2003年利用RSA和Fiat-Shamir身份鉴别方案首次提出了基于ID的一次性盲公钥技术[4],其结合基于身份的密码系统,引入双线性对运算构造了一种基于身份的一次性公钥方案。文献[1,6-7]对该方案进行了安全性分析,发现其签名过程可伪造,并提出了改进方案。然而上述方案中私钥完全由第三方生成,一旦第三方被恶意用户攻破或者获得了系统主密钥,用户的通信将不存在任何机密性,针对该问题,文献[8]提出了改进方案。上述一次性公钥方案的安全性均建立在第三方完全诚实可信的前提条件下,如果第三方主动将用户的私钥泄露给恶意用户,帮助其伪造出“合法私钥”或者自身充当恶意用户伪造秘密值,将伪造私钥绑定到同一用户,然后泄露给敌手,用户将面临签名伪造的安全风险[10,12]。为此,研究者对降低第三方信任度的私钥生成方案展开了研究,其中一种方法是采用分布式的方式将单个机构的信任分散到多个机构,通过引入多个密钥托管方生成有效私钥[11-12],然而这种方法需要为每个机构设置安全信道,增

到稿日期:2017-05-18 返修日期:2017-07-24 本文受河南省基础与前沿技术研究计划(142300413201)资助。

柴林鹏(1993-),男,硕士生,主要研究方向为身份认证,E-mail:chailinpeng126@126.com;张 斌(1969-),男,教授,主要研究方向为网络空间安全,E-mail:zhangb1969@sohu.com(通信作者)。

大了系统的通信和计算开销;另一种方法借鉴了 Goyal 等的可追踪审计思想[13],提出了具有审计功能的签名加密方案[14-15],用户可通过提交自身的私钥揭示第三方的恶意行为,有效约束了第三方的不诚实行为,然而该类方案从用户诚实可靠的角度出发,并未考虑用户匿名性以及第三方对恶意用户的追踪。

本文提出一种可抵抗不诚实第三方攻击的一次性公钥改进方案,结合文献[17]提出的基于身份的签名算法,利用用户私钥建立与用户身份唯一对应的身份索引,将私钥生成过程中与用户真实身份无关的部分信息作为公开可验证信息进行发布。用户与服务提供方分别通过完整私钥的正确性验证以及与身份索引唯一对应的公开可验证信息的正确性判定两种方式来对第三方行为进行双重约束。利用索引生成算法为每个用户建立唯一的身份索引,在追踪恶意用户时不需要对所有用户进行运算开销比较大的双线性对运算,将双线性对运算减少到一次,以进一步提高追踪效率。

2 预备知识

2.1 双线性映射

设 G_1 和 G_2 是两个 q 阶的循环群,其中 q 是一个大素数。将 G_1 定义为有限域 F_p 中椭圆曲线上的一个点群,G_2 是定义在 $F_{q^2}^*$ 上的一个子群。因此可以将 G_1 定义为一个阶数为 q 的加法循环群,其生成元为 P,将 G_2 定义为一个阶数为 q 的乘法循环群[18],定义双线性映射 $e:G_1\times G_1\rightarrow G_2$,其性质如下。

1)双线性:对于任意 $M,N\in G_1$,$v,w\in Z_q^*$,均有 $e(vM,wN)=e(M,N)^{vw}$。

2)非退化性:对于生成元 $P\in G_1$,$e(P,P)\neq 1$,其中 1 是 G_2 的单位元。

3)可计算性:存在有效算法计算 $e(M,N)$。

2.2 困难假设

方案的安全性基于以下困难数学问题。

1)离散对数问题(DLP):给定 $M,N\in G_1$,找到一个整数 $n\in Z_q^*$,满足 $N=nM$。

2)计算性 Diffie-Hellman 问题(CDHP):设 $v,w\in Z_q^*$,给定 $P,vP,wP\in G_1$,计算 $vwP\in G_1$。

3)双线性 Diffie-Hellman 问题(BDHP):设 $v,w,z\in Z_q^*$,给定 $P,vP,wP,zP\in G_1$,计算 $e(P,P)^{vwz}\in G_2$。

3 抗不诚实第三方攻击的一次性公钥方案及其安全性分析

3.1 抗不诚实第三方攻击的一次性公钥方案

1)系统初始化

第三方 TP 设置安全参数 λ,$q\geqslant 2^{\lambda}$ 为素数,将 G_1 和 G_2 分别定义为一个 q 阶的加法群和乘法群,G_1 的生成元为 P,Z_q 为 q 阶的有限域。定义双线性映射 $e:G_1\times G_1\rightarrow G_2$,随机选择 $s\in Z_q^*$ 作为系统主密钥,其中 $Z_q^*=Z_q\setminus\{0\}$,系统公钥为 $Q_{TP}=sP$。选择 4 个防碰撞散列函数[19] $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\times G_1\rightarrow Z_q^*$,$H_3:G_2\rightarrow Z_q^*$,$H_4:\{0,1\}^*\times G_1\times G_1\rightarrow Z_q^*$。TP 妥善保管 s,公开系统参数$\{G_1,G_2,e,q,P,Q_{TP},H_1,H_2,H_3,H_4\}$。

2)用户私钥生成

①身份标识为 ID_u 的用户 u 随机选择秘密值 $x_u\in Z_q^*$,计算 $R_1=x_uP$,将(ID_u,R_1)发送至 TP。

②TP 收到消息后,在恶意用户列表中对 ID_u 进行查询,如果检测到该用户,则停止后续操作。完成对用户身份合法性鉴定后,TP 计算 $r_u=H_2(sQ_u)$,$R_2=r_uP$,其中 $Q_u=H_1(ID_u)$,$R_u=R_1+R_2$,部分私钥 $D_u=r_u+s$,并生成用户身份索引 $ind_u=H_3(e((R_1+D_uP),P))$。将 R_u 作为公开可验证信息。

TP 在用户列表中保存(ind_u,ID_u),并在公开列表中发布信息(ind_u,R_u),将(ind_u,D_u)通过安全通道发送至用户 u。

③用户 u 计算完整私钥 $S_u=x_u+D_u$,并结合公开列表中的 R_u 验证 $S_uP=R_u+Q_{TP}$ 是否成立,验证通过后安全保存(S_u,R_u)。

3)用户一次性公钥生成

用户选取随机数 $a\in Z_q^*$,计算一次性公钥 $Q_u=(Q_1,Q_2,Q_3)$,其中 $Q_1=aS_uP$,$Q_2=aR_u$,$Q_3=aP$。

4)消息签密

①假设用户 u 与服务提供方 SP 进行通信,基于无证书密码体制思想,SP 在 TP 中心进行注册。

SP 随机选取 $x_{SP}\in Z_q^*$,计算自身公钥 $PK_{SP}=x_{SP}P$,将消息(PK_{SP},ID_{SP})发送至 TP 进行服务注册,并向 TP 零知识证明 SP 拥有随机数 x_{SP}。TP 计算 $Q_{SP}=H_1(ID_{SP})$,$D_{SP}=sQ_{SP}$,将部分私钥 D_{SP}安全发送至 SP;SP 生成完整私钥 $S_{SP}=(D_{SP},x_{SP})$。

②用户向 SP 发送请求消息 Msg,用户随机选择 $b\in Z_q^*$,令 $t=H_3(e(Q_{SP},Q_{TP})^b)$,计算 $c_1=bP$,$h=H_4(c_1,t,bPK_{SP})$,$c_2=Msg\oplus h$,$\delta=S_u/(h+b)$,将(Q_u,c_1,c_2,δ)发送至 SP。

5)一次性公钥验证及解密验签

SP 接收到消息后,首先验证一次性公钥的合法性,即验证等式

$$e(Q_1,P)=e(Q_2,P)e(Q_3,Q_{TP}) \tag{1}$$

是否成立,然后利用自己的私钥解密验签,计算 $t=H_3(e(D_{SP},c_1))$,$h=H_4(c_1,t,x_{SP}c_1)$,获得请求消息 $Msg=c_2\oplus h$。

证明:

$$\begin{aligned}t&=H_3(e(Q_{SP},Q_{TP})^b)\\&=H_3(e(Q_{SP},bQ_{TP}))\\&=H_3(e(Q_{SP},bsP))\\&=H_3(e(sQ_{SP},bP))\\&=H_3(e(D_{SP},c_1))\end{aligned}$$

$$\begin{aligned}e(Q_1,P)&=e(aS_uP,P)\\&=e(a(x_u+D_u)P,P)\\&=e(a(x_u+r_u+s)P,P)\\&=e(a(x_u+r_u)P,P)e(asP,P)\\&=e(aR_u,P)e(aP,Q_{TP})\\&=e(Q_2,P)e(Q_3,Q_{TP})\end{aligned}$$

若成立,SP 可以确定一次性公钥中包含系统主密钥,即用户在第三方进行了注册;否则放弃消息。然后验证等式

$$e(\delta Q_3,hP+c_1)=e(Q_1,P) \tag{2}$$

是否成立,验证通过后接收消息。

证明：

$$\begin{aligned}e(\delta Q_3, hP+c_1) &= e(S_u Q_3/(h+b), hP+c_1)\\ &= e(S_u Q_3/(h+b), (h+b)P)\\ &= e(aS_uP, P)\\ &= e(Q_1, P)\end{aligned}$$

在安全级别比较高的应用场景中，可进一步根据与身份索引唯一对应的公开可验证信息的正确性来判定用户是否遭受不诚实 TP 的恶意攻击。通过计算 $ind_u = H_3(e(\delta P, hP+c_1))$，并在公开列表中查找相应的身份索引，获取相应的公开可验证消息 R_u，验证等式

$$e(Q_2, P) = e(R_u, Q_3) \tag{3}$$

是否成立。若成立，则表明用户未遭受不诚实 TP 的恶意攻击；否则，放弃消息。

证明：

$$\begin{aligned}H_3(e(\delta P, hP+c_1)) &= H_3(e(S_uP/(h+b), (h+b)P))\\ &= H_3(e(S_uP, P))\\ &= ind_u\end{aligned}$$

3.2　方案安全性分析

3.2.1　发送方具有匿名性

首先，用户采用随机数 a 对公钥进行处理，通过对式(1)的验证只能确定用户在 TP 进行了注册，属于合法用户，但是无法从用户的一次性公钥中得到任何与用户有关的身份信息，确保了用户身份信息免遭泄露，且随机数的选取使得合法用户的会话行为对于外部用户具有不可关联性，确保了用户行为免遭统计分析。其次，用户请求消息的签密信息为 (c_1, c_2, δ)，对信息的解密验签需要用到 SP 的私钥 (D_{SP}, x_{SP})，保证了消息传输的机密性，防止外部用户从会话内容中分析出与用户有关的身份信息。

3.2.2　一次性公钥和签密不可伪造

一次性公钥的不可伪造性可分为未注册用户和合法用户两种情况进行讨论。对于未注册过的用户而言，可通过两种方式伪造一次性公钥：1)结合公共参数选择任意随机数 $m, n \in Z_q^*$，生成可满足式(1)的一次性公钥 $Q_1' = mP + nQ_{TP}$，$Q_2' = mP$，$Q_3' = nP$，但是其无法获得系统主密钥，进而无法计算出签密私钥 $m+ns$，同时也无法伪造出能够通过式(2)验证的合法签名 δ；2)利用合法用户的一次性公钥信息 Q_u 进行伪造，选取随机数 $c \in Z_q^*$，生成可通过式(1)验证的 $Q_u' = (cQ_1, cQ_2, cQ_3)$，然而敌手依然无法获得签密私钥 S_u，因为通过 $Q_1 = aS_uP$ 和 $Q_3 = aP$ 获得 S_u 面临椭圆曲线 DLP 问题。

对于注册过的合法用户来说，伪造一次性公钥的目的是躲过式(4)的追踪，以消除自己恶意活动的证据。假设用户选择随机数 $m, n \in Z_q^*$，生成可满足式(1)的一次性公钥 $Q_1' = mR_u + nQ_{TP}$，$Q_2' = mR_u$，$Q_3' = nP$，同时躲过了式(4)的追踪，但是用户无法生成合法签名，因为 $m(x_u + r_u)P$ 和 sP 求解签名私钥 $m(x_u + r_u) + ns$ 面临椭圆曲线群上 DLP 问题。因此，即使是合法用户也无法伪造出合法的一次性公钥及签密。

由于签密信息的不可伪造性，敌手无法根据本次通信消息 (c_1, c_2, δ) 进行签密伪造。假设伪造消息 (c_1', c_2', δ') 满足式(1)和式(2)，其中 $h = H_4(c_1', t', c'PK_{SP})$。对于伪造的签密 δ'，若使选取的随机数 $y \in Z_q^*$，需要以下两个条件之一成立：1)$\delta' Q_3 = yQ_1 \wedge H_4(c_1', t', c'PK_{SP})P + c_1' = y^{-1}P$；2)$\delta' Q_3 = yP \wedge H_4(c_1', t', c'PK_{SP})P + c_1' = y^{-1}Q_1$，以条件 1)为例，非法用户需要计算 c'，使其满足 $c_1' = y^{-1}P - H_4(c_1', t', c'PK_{SP})P$，但是 H_4 是单向函数，所以非法用户无法获得满足条件的 c_1'，因此条件 1)不成立，同理可证条件 2)不成立。

3.2.3　签密的安全性

在改进的一次性公钥方案中，使用到了双线性对 $e(Q_{SP}, Q_{TP})^b$ 以及根据随机数生成的 $c_1 = bP$，$h = H_4(c_1, t, bPK_{SP})$，因此只有指定的消息接收者利用自己的私钥 (D_{SP}, x_{SP}) 才能恢复出正确的请求消息 Msg，实现对消息的解密验签，与文献[1,4-7]相比，增加了通信消息的机密性。

3.2.4　密钥托管问题

依据上文分析，密钥托管问题主要分为两个方面：

1)在 TP 完全诚实可信的前提下，针对恶意用户获得系统主密钥后可计算出用户的合法签名密钥的问题，改进方案中 TP 只负责生成部分私钥，由用户结合随机数 x_u 生成完整私钥 $S_u = x_u + D_u$，其中 x_u 是用户自行选择的秘密值，其他用户及 TP 均无法获得 x_u。因此，即使恶意用户获得了 TP 的主密钥 s，依然无法生成用户的完整私钥。

对于 SP 来说，其公私钥的生成利用了无证书密码体制思想，其私钥为 $S_{SP} = (D_{SP}, x_{SP})$，其中 D_{SP} 由 TP 根据用户的身份 ID_{SP} 以及系统主密钥 s 计算生成，安全发送到用户后，由用户选取随机数生成完整私钥，确保了第三方无法获得 SP 的完整私钥。

2)假设 TP 不诚实，且存在主动发起恶意攻击的行为，不诚实 TP 的攻击可分为消极不诚实级攻击和积极不诚实级攻击[16]。

通过引入公开列表的方式，将与用户的身份信息无关的 R_u 作为公开可验证信息，保证用户选取的秘密值成为完整私钥的前置条件。如果消极不诚实级的 TP 发起伪造攻击，将用户的部分私钥泄露给敌手，那么敌手可自行选取随机数 $x_u' \in Z_q^*$，进而伪造用户完整私钥 $S_u' = x_u' + D_u$，实施假冒攻击。由于 TP 将 R_u 发布到公开列表中，SP 可以通过验证身份索引的存在性来确定用户是否遭到了不诚实 TP 攻击，即 SP 依据签密消息计算用户的身份索引 $ind_u' = H_3(e(\delta' P, h'P + c_1'))$，在 TP 的公开列表中遍历身份索引，如果不存在该索引，则放弃消息，如果存在该身份索引，则进一步验证式(3)是否成立。

如果用户遭受到积极不诚实 TP 攻击，其冒充用户将公开列表中的 (ind_u, R_u) 进行替换，并将伪造的完整私钥泄露给敌手，那么用户可结合公开列表中的 R_u' 来验证 $S_uP = R_u' + Q_{TP}$ 是否成立，从而判断其是否遭到积极不诚实的 TP 攻击。

3.2.5　恶意用户可追踪性

如果 SP 发现用户存在恶意行为，可通过与 TP 合作来揭示用户的真实身份。SP 向 TP 提交证据 (δ, c_1, h)，TP 计算：

$$ind_u = H_3(e(\delta P, hP + c_1)) \tag{4}$$

并根据账户列表(ind_u,ID_u)中的身份索引 ind_u 进行遍历搜索,从而获取恶意用户的身份 ID_u。

3.3 方案效率分析

本节将对方案的计算、通信开销以及追踪效率进行分析,并与文献[1,8-9]中的方案进行比较,结果如表 1 所列。运算开销中只需要考虑双线性对运算(Pa)、G_1 上的点乘运算(Pm)、G_1 上的点加运算(Ad)、G_2 上的点乘运算(Gm)、椭圆曲线上的哈希运算(MtP)、指数运算(Em)。T_0,T_1,T_8,T_9 分别表示不同方案对单个恶意用户追踪的时间开销,l 表示恶意用户的数量,k 表示已注册用户的数量,其他运算可忽略不计。由表 1 中可以看出,本方案在对消息进行签密时具有更小的计算开销以及更高的传输效率。同时,在追踪恶意用户时,分为两种情况进行比较:1)在追踪单个恶意用户时,本文方案将运算开销比较大的双线性对运算减少到一次,因此 4 个方案的时间消耗为 $T_1 > T_8 = T_9 > T_0$;2)在追踪多个恶意用户时,身份索引算法为用户建立了唯一的索引,其追踪过程中不需要对所有用户进行遍历运算,与其他方案相比具有更高的追踪效率。

表 1 不同方案的效率比较

Table 1 Efficiency comparison of different schemes

密码算法	文献[1]	文献[8]	文献[9]	本文方案
生成一次性公钥	5Pm	3Pm	3Pm	3Pm
收方验证公钥	7Pa+Gm	3Pa+Gm	3Pa+Gm	3Pa+Gm
收方验证签名(密)	2Pa+Em	2Pm+Ad+MtP	2Pm+Ad+MtP	Pa+Pm+MtP
一次性公钥长度	G_1^5	G_1^3	G_1^3	G_1^3
单个恶意用户追踪	3Pa+Pm+Gm	2Pa+Pm	2Pa+Pm	Pa+2Ad+MtP
多个恶意用户追踪	$k\times l\times T_1$	$k\times l\times T_8$	$k\times l\times T_9$	$l\times T_0$

结束语 本文分析了现有典型的一次性公钥方案,指出方案的安全性建立在第三方完全诚实可信的基础上,无法抵抗不诚实第三方的恶意攻击。在改进的一次性公钥方案中,建立与身份信息唯一对应的身份索引,并发布与用户真实身份无关的公开可验证信息。用户通过完整私钥的正确性验证来防止积极不诚实级第三方的恶意攻击;服务提供方通过签密信息获取用户身份索引,并判定其与相应的公开可验证信息的正确性,从而阻止消极不诚实第三方的恶意行为。同时,采用的索引生成算法将双线性对运算次数减少到一次,且不需要对所有用户进行遍历运算,提高了对恶意用户的追踪效率。下一步工作将在该方案的基础上考虑与用户的访问控制相结合,设计能够支持细粒度访问控制的匿名认证协议。

参 考 文 献

[1] LI Y,ZHANG S W,ZHANG Y Y. Analysis and improvementation on identity-based one-off public key[J]. Computer Engineering and Design,2008,29(7):1636-1637,1640. (in Chinese)
李毅,张少武,张远洋. 基于身份一次性公钥的分析与改进[J]. 计算机工程与设计,2008,29(7):1636-1637,1640.

[2] ZHU X L,LU Y,ZHANG B H,et al. Efficient Fair Pseudonym Management Model[J]. Computer Science,2013,40(11):122-125. (in Chinese)
朱晓玲,陆阳,张本宏,等. 一种公平有效的假名管理模型[J]. 计算机科学,2013,40(11):122-125.

[3] LU J,SONG X M,HAN M,et al. Batch Verification Scheme Defensing Coliusive Attack in VANET[J]. Computer Science,2016,43(6):135-140. (in Chinese)
陆杰,宋香梅,韩牟,等. 车载网中可抵制合谋攻击的批量认证方案[J]. 计算机科学,2016,43(6):135-140.

[4] ZHANG Q P,GUO B A. One-off Blind Public Key Based on ID[J]. Acta Electronica Sinica,2003,31(5):769-771. (in Chinese)
张秋璞,郭宝安. 基于 ID 的一次性盲公钥[J]. 电子学报,2003,31(5):769-771.

[5] ZHANG S,XU G A,HU Z M,et al. Construction of the One-off Public Key Based on Identity[J]. Journal of Electronics & Information Technology,2006,28(8):1412-1414. (in Chinese)
张胜,徐国爱,胡正名,等. 一种基于身份一次性公钥的构造[J]. 电子与信息学报,2006,28(8):1412-1414.

[6] LU R B,HE D K,WANG C J. Improvement on one-off public key based on identity[J]. Application Research of Computers,2008,25(4):1139-1141. (in Chinese)
鲁荣波,何大可,王常吉. 改进的基于身份的一次性公钥[J]. 计算机应用研究,2008,25(4):1139-1141.

[7] ZHEN H H,CHEN Y,LI L,et al. Analysis and Reproduction of One-off Public Key[J]. Computer Engineering,2010,36(1):187-188,196. (in Chinese)
甄鸿鹄,陈越,李乐,等. 基于身份的一次性公钥分析与重构[J]. 计算机工程,2010,36(1):187-188,196.

[8] LUO C Y,HUO S W,XING H Z,et al. Anonymous authentication scheme based on one-off public key in pervasive computing environments[J]. Journal on Communications,2012,33(2):93-98,109. (in Chinese).
罗长远,霍士伟,邢洪智,等. 普适环境中基于一次性公钥的匿名认证方案[J]. 通信学报,2012,33(2):93-98,109.

[9] ZHOU Y W,YANG B. Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things[J]. Journal of Software,2015,26(9):2436-2450. (in Chinese)
周彦伟,杨波. 物联网移动节点直接匿名漫游认证协议[J]. 软件学报,2015,26(9):2436-2450.

[10] WANG Z H. Research on Several Security Mechanisms for Cloud Storage Service[D]. Beijing:Beijing Jiaotong University,2016. (in Chinese)
王中华. 云存储服务的若干安全机制研究[D]. 北京:北京交通大学,2016.

[11] ZHANG C S,WANG S P,YAO S W,et al. A Key Escrow Scheme to Identify Cheaters Based on PKI[J]. Computer Science,2005,32(11):72-74,80. (in Chinese)
张春生,王世普,姚绍文,等. 基于 PKI 防欺诈的门限密钥托管方案[J]. 计算机科学,2005,32(11):72-74,80.

(下转第 185 页)

Data Engineering，2013，25(2)：274-284.

[6] HU Q H，YU D R，XIE Z X. Information-preserving hybrid data reduction based on fuzzy-rough techniques[J]. Pattern Recognition Letters，2006，27(5)：414-423.

[7] MIAO D Q，ZHAO Y，YAO Y Y，et al. Relative reducts in consistent and inconsistent decision tables of the Pawlak rough set model[J]. Information Sciences，2009，179(24)：4140-4150.

[8] JIA X Y，SHANG L，ZHOU B，et al. Generalized attribute reduct in rough set theory[J]. Knowledge-Based Systems，2016，91(C)：204-218.

[9] LEUNG Y，FISCHER M M，WU W Z，et al. A rough set approach for the discovery of classification rules in interval-valued information systems[J]. International Journal of Approximate Reasoning，2008，47(2)：233-246.

[10] YANG X B，QI Y，YU D J，et al. α-Dominance relation and rough sets in interval-valued information systems[J]. Information Sciences，2015，294(5)：334-347.

[11] XU F F，BI Z Q，LEI J S. Approximate reduction for the interval-valued decision table[M] // Rough Sets and Knowledge Technology. Springer International Publishing，2014：89-100.

[12] ZHANG N，MIAO D Q，YUE X D. Approach-es to knowledge reduction in interval-valued information systems[J]. Journal of Computer Research and Development，2010，47(8)：1362-1371. (in Chinese)
张楠，苗夺谦，岳晓冬. 区间值信息系统的知识约简[J]. 计算机研究与发展，2010，47(8)：1362-1371.

[13] LIU P H，CHEN Z C，QIN K Y. Decision attribute reduction of interval-valued informa-tion systems[J]. Computer Engineering and Applications，2009，45(28)：148-150. (in Chinese)
刘鹏惠，陈子春，秦克云. 区间值信息系统的决策属性约简[J]. 计算机工程应用，2009，45(28)：148-150.

[14] DU W S，HU B Q. Approximate distribution reducts in inconsistent interval-valued ordered decision tables[J]. Information Sciences，2014，271(7)：93-114.

[15] ZHANG N，XU X，TONG X R，et al. Knowledge reduction in inconsistent interval-valued decision systems[J]. Journal of Chinese Computer Systems，2017，38(7)：1585-1589. (in Chinese)
张楠，许鑫，童向荣，等. 不协调区间值决策系统的知识约简[J]. 小型微型计算机系统，2017，38(7)：1585-1589.

[16] DAI J H，WEI B，ZHANG X，et al. Uncertainty measurement for incomplete interval-valued information systems based on α-weak similarity[J]. Knowledge-Based Systems，2017，136(11)：159-171.

[17] BAGGENSTOSS P M. Class-specific feature sets in classification[J]. IEEE Transactions on Signal Processing，1999，47(12)：3428-3432.

[18] CHEN D G，ZHAO S Y. Local reduction of decision system with fuzzy rough sets[J]. Fuzzy Sets & Systems，2010，161(13)：1871-1883.

[19] YAO Y Y，ZHANG X Y. Class-specific attribute reducts in rough set theory[J]. Information Sciences，2017，418(38)：601-618.

[20] JU H R，LI H X，ZHOU X Z，et al. Spquential three-way classifier with local reduction[J]. Computer Science，2017，44(9)：34-39. (in Chinese)
鞠恒荣，李华雄，周献中，等. 基于 Local 约简的序贯三支分类器[J]. 计算机科学，2017，44(9)：34-39.

[21] QIAN Y H，LIANG X Y，LIANG J Y，et al. Local rough set：a solution to rough data analysis in big data[J]. International Journal of Approximate Reasoning，2018，97(6)：38-63.

[22] LIU G L，HUA Z，ZOU J Y. Local attribute reductions for decision tables[J]. Information Sciences，2017，422：204-217.

[23] ZHANG X，MEI C L，CHEN D G，et al. Multi-confidence rule acquisition and confidence-preserved attribute reduction in interval-valued decision systems[J]. International Journal of Approximate Reasoning，2014，55(8)：1787-1804.

(上接第 142 页)

[12] CAO D，WANG X F，WANG F，et al. SA-IBE：A Secure and Accountable Identity-based Encryption Scheme[J]. Journal of Electronic & Information Technology，2011，33(12)：2922-2928. (in Chinese)
曹丹，王小峰，王飞，等. SA-IBE：一种安全可追责的基于身份加密方案[J]. 电子与信息学报，2011，33(12)：2922-2928.

[13] GOYAL V. Reducing trust in the PKG in identity based cryptosystem[C] // Advances in Crytology-CRYPTO 2007. Springer Berlin Heidelberg，2007：430-447.

[14] REN Y. Attribute-based Signature with Audita - biling in Standard Model[J]. Computer Science，2015，42(2)：142-146. (in Chinese)
任燕. 标准模型下可审计的基于属性的签名方案[J]. 计算机科学，2015，42(2)：142-146.

[15] LONG Y，XU X，CHEN K F. Two Identity Based Threshold Cryptosystem with Reduced Trust in PKG[J]. Journal of Computer and Development，2012，49(5)：932-938. (in Chinese)
龙宇，徐贤，陈克非. 两个降低 PKG 信任级的基于身份的门限密码体制[J]. 计算机研究与发展，2012，49(5)：932-938.

[16] FAN A W，YANG Z F，XIE L M，et al. Security analysis and improvement of strongly secure certificateless signature scheme[J]. Journal on Communications，2014，35(5)：118-123. (in Chinese)
樊爱宛，杨照峰，谢丽明，等. 强安全无证书签名方案的安全性分析和改进[J]. 通信学报，2014，35(5)：118-123.

[17] CAO X F，ZENG X W，KOU W D，et al. A novel anonymous authentication scheme over the insecure channel[J]. Journal of Xidian University，2007，34(6)：877-880，910. (in Chinese)
曹雪菲，曾兴雯，寇卫东，等. 一种新的不安全信道上的匿名认证方案[J]. 西安电子科技大学学报(自然科学版)，2007，34(6)：877-880，910.

[18] DAN B，MATT F. Identity-Based Encryptionfrom the Weil Pairing[J]. Lecture Notes in Computer Science，2001，2139(1)：213-229.

[19] NIST. Secure Hash Standard(SHS)[EB/OL]. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.