部分盲签名综述*

李明祥[1,2]，李 峰[1]，王 涛[1]
(1. 河北金融学院 信息管理与工程系，河北 保定 071051；2. 河北省科技金融重点实验室，河北 保定 071051)

摘 要：首先叙述了部分盲签名在传统公钥密码体制下的研究现状，并介绍了一个有代表性的部分盲签名方案；然后叙述了部分盲签名在基于身份的密码体制下的研究进展，同时介绍了一个典型的基于身份的部分盲签名方案；随后叙述了部分盲签名在无证书公钥密码体制下的研究现状，介绍了一个有代表性的无证书部分盲签名方案；最后说明了部分盲签名目前存在的问题，并指出了下一步的研究方向。

关键词：部分盲签名；基于身份；无证书；双线性对
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2012)12-4437-04
doi:10.3969/j.issn.1001-3695.2012.12.007

Survey of partially blind signature

LI Ming-xiang[1,2], LI Feng[1], WANG Tao[1]
(1. *Dept. of Information Management & Engineering, Hebei Finance University, Baoding Hebei* 071051, *China*; 2. *Hebei Science & Technology Financial Critical Laboratory, Baoding Hebei* 071051, *China*)

Abstract: At first, this paper described the research situation of partially blind signature under the traditional public key cryptography, and introduced a representative of the partially blind signature schemes. Then it discussed the progresses of partially blind signature under the identity-based cryptography, and introduced a typical identity-based partially blind signature scheme. Then it described the advances of partially blind signature under the certificateless public key cryptography, and introduced a representative certificateless partially blind signature scheme. Finally, it illustrated the existing problems of partially blind signature, and pointed out the future research directions.

Key words: partially blind signature; identity-based; certificateless; bilinear pairings

1982 年 Chaum[1] 首先提出了盲签名的概念。在盲签名中用户可获得签名人的签名，而签名人却不知道所签消息的内容。盲签名可广泛应用于各种关注匿名性的场合，如电子现金、电子投票等。不过在盲签名中签名人完全不知道最终签名的任何信息，将在电子现金系统中造成数据库无限增长等问题。为了解决这些问题，1996 年 Abe 等人[2] 又提出了部分盲签名的概念。部分盲签名允许签名人在签名中嵌入与用户事先协商好的公共信息，而且这些公共信息不能被移除或非法修改。在电子现金系统中，银行可将有效期、面值等信息嵌入到其发行的电子钱币中，这样银行就能避免维持开销无限增长的数据库的困境。如果将公共信息设为同样的值，则部分盲签名就可以转换为完全盲签名。因此，部分盲签名可看做盲签名的一般形式。鉴于部分盲签名在电子现金、电子投票等领域的广阔应用前景，使它受到了国内外学者的广泛关注。

目前，人们已提出了不少各具特色的部分盲签名方案。由于数字签名是公钥密码体制的特有应用，因此以公钥密码体制为序综述部分盲签名的研究进展。

1 基于 PKI 的部分盲签名研究

1.1 研究现状

1976 年 Diffie 等人[3] 提出了公钥密码体制的思想。在公钥密码体制架构下，每个用户都拥有一对匹配的密钥，即公钥与私钥，由此公钥密码体制不仅能实现加密功能，还能实现认证功能。根据这一思想，人们基于大数分解问题提出了 RSA 等公钥密码体制，基于离散对数问题提出了 ElGamal 等公钥密码体制。在这些公钥密码体制中，用户的公钥与其身份没有任何联系。为此，需要建立公钥基础设施(PKI)，通过证书机构(CA)为用户签发的公钥证书将用户的身份与其公钥联系起来。不过这种方式的证书管理过程需要很高的计算开销和存储开销。

2000 年 Abe 等人[4] 根据盲签名的安全特性，即盲性与不可伪造性[5]，定义了部分盲签名的安全特性，即部分盲性和不可伪造性，并且基于离散对数问题提出了一个可证安全的部分盲签名方案。2007 年 Wu 等人[6] 基于离散对数问题又提出了一个高效的可证安全的部分盲签名方案。2005 年 Cao 等人[7] 基于大数分解问题提出了一个部分盲签名方案。可是 2006 年 Martinet 等人[8] 指出 Cao 方案是不安全的，攻击者能够伪造有效的部分盲签名。2004 年 Huang 等人[9] 提出了一个高效的部分盲签名方案。然而 2005 年 Zhang 等人[10] 指出 Huang 方案存在安全缺陷，恶意用户能够随意修改事先协商的公共信息。2003 年 Zhang 等人[11] 基于双线性对提出了一个部分盲签名方案。2005 年 Chow 等人[12] 基于双线性对又提出了一个部分盲签名方案。对用户来说，Chow 部分盲签名方案比 Zhang 部分

收稿日期：2012-04-20；**修回日期**：2012-05-30 **基金项目**：国家“973”重点基础研究发展规划基金资助项目(2011CB311809)；国家自然科学基金面上项目(61163050)

作者简介：李明祥(1968-)，男，山东济宁人，副教授，博士，主要研究方向为公钥密码学及其应用(limingxiang2008@gmail.com)；李峰(1981-)，男，讲师，硕士，主要研究方向为金融信息安全技术；王涛(1973-)，副教授，硕士，主要研究方向为信息系统设计与分析.

盲签名方案要高效一些。另外,2006 年 Okamoto[13] 提出了一个在标准模型下可证安全的部分盲签名方案。下面具体介绍一下 Zhang 部分盲签名方案[11]。

1.2 Zhang 部分盲签名方案

1)方案描述

a)建立。选择阶为 q 的循环群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$,定义双线性对 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$;任意选择群 $\mathbb{G}_1$ 的生成元 P;定义两个密码哈希函数 $H_1:\{0,1\}^*\to\mathbb{G}_1$, $H_2:\{0,1\}^*\to\mathbb{Z}_q^*$。系统参数为 params = $\{\mathbb{G}_1,\mathbb{G}_2,e,q,P,H_1,H_2\}$。

b)密钥生成。签名人任意选择 $x\in\mathbb{Z}_q^*$,计算 $P_{pub}=xP$。其中:签名人的公钥为 P_{pub},私钥为 x。

c)签名发布。假设 c 为事先协商好的公共信息,则签名人与用户的交互过程如下:

(a)盲化。用户随机选择 $r\in\mathbb{Z}_q^*$,计算 $U=rH_1(m,c)$,并将 U 发送给签名人。

(b)签名。签名人计算 $V=(H_2(c)+x)^{-1}U$,并把 V 发送给用户。

(c)解盲。用户计算 $S=r^{-1}V$,并输出部分盲签名(S,m,c)。

d)签名验证。检查下列等式:

$$e(H_2(c)P+P_{pub},S)=e(P,H_1(m,c))$$

是否成立。若成立则接受该签名,否则拒绝该签名。

2)性能评价

Zhang 等人严格证明了该方案的部分盲性与不可伪造性。其在签名发布时无须作双线性对运算,在签名验证时仅需作两次双线性对运算。双线性对运算是比较耗时的,因此 Zhang 方案是相当高效的。另外易见,Zhang 方案的签名长度是非常短的。由于在电子现金系统中,用户的计算资源和存储资源很有限,因此 Zhang 方案在电子现金系统中具有良好的应用前景。

2 基于身份的部分盲签名研究

2.1 研究现状

1984 年 Shamir[14] 提出了基于身份的密码体制的概念。在这种密码体制架构下,用户的身份信息即是用户的公钥,从而把用户的身份与其公钥以一种自然的方式捆绑在了一起,因此基于身份的公钥密码体制克服了因管理公钥证书而产生的效率瓶颈。由于所有用户的私钥都是由私钥生成器(PKG)利用主秘密值产生的,因此基于身份的密码系统存在密钥托管问题。基于身份的密码学的研究进展可参阅文献[15]。

2005 年 Chow 等人[12] 定义了一个基于身份的部分盲签名的安全模型,并提出了一个可证安全的基于身份的部分盲签名方案;另外 Chow 等人还提出了窜改协商信息攻击的概念。窜改协商信息攻击是一种伪造攻击,它是指用户在获得签名人发布的签名后擅自修改协商信息,而部分盲签名仍是有效的。

2007 年 Hu 等人[16] 提出了一个高效的基于身份的部分盲签名方案,并在 Chow 等人定义的安全模型下证明了所提方案的不可伪造性。然而 Tseng 等人[17] 指出 Hu-Huang 方案[16] 存在窜改协商信息攻击。窜改协商信息攻击的存在说明 Chow 等人[12] 定义的安全模型是不完善的。

Chow-Hui 模型究竟不完善在什么地方呢? 在 Chow-Hui 模型中,挑战者在回答敌手的签名询问时,签名发布协议是由挑战者单方执行的,而不是由挑战者与敌手两方交互执行,这是不符合实际情况的。例如,当用户发起窜改协商信息攻击时,签名发布协议是由签名人与用户两方交互执行的。因此 Chow-Hui 模型不能俘获基于身份的部分盲签名方案遭受的窜改协商信息攻击。

2007 年张学军等人[18] 又提出了一个高效的基于身份的部分盲签名方案。可是闫东升[19] 指出张—王方案[18] 也存在窜改协商信息攻击。同时闫东升[19] 还提出了一个基于身份的部分盲签名方案。不过闫方案没有提供严格的安全性证明。2008 年崔巍等人[20] 又提出了一个基于身份的部分盲签名方案。但是李明祥等人[21] 指出崔—辛方案[20] 不能抵抗窜改协商信息攻击。最近李明祥等人[22] 也提出了一个基于身份的部分盲签名方案。不过李—郑方案[22] 是在 Chow-Hui 模型下完成其安全性证明的。下面具体介绍一下 Chow-Hui 基于身份的部分盲签名方案。

2.2 Chow-Hui 基于身份的部分盲签名方案

1)方案描述

a)建立。PKG 选择阶为 q 的循环群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$,定义双线性对 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$;任意选择群 $\mathbb{G}_1$ 的生成元 P,随机选择$s\in\mathbb{Z}_q^*$,计算 $P_{pub}=sP$;选取两个密码哈希函数 $H_1:\{0,1\}^*\to\mathbb{G}_1$, $H_2:\{0,1\}^*\to\mathbb{Z}_q^*$。系统参数为 params = $\{\mathbb{G}_1,\mathbb{G}_2,e,q,P,P_{pub},H_1,H_2\}$,主秘密值为 s。

b)密钥产生。签名人向 PKG 提交其身份 ID,PKG 设定签名人的公钥为 $Q_{ID}=H_1(ID)$,私钥为 $S_{ID}=sQ_{ID}$,并将 S_{ID} 通过安全信道发送给签名人。

c)签名发布。假设 c 为事先协商好的公共信息,则用户与签名人的交互过程如下:

(a)签名(阶段 1)。签名人随机选择 $r\in\mathbb{Z}_q^*$,计算 $C=rP$, $Y=rQ_{ID}$,并将(Y,C)发送给用户。

(b)盲化。用户随机选择 $\alpha,\beta,\gamma\in\mathbb{Z}_q^*$,计算 $Y'=\alpha Y+\alpha\beta Q_{ID}-\gamma H_1(c)$, $C'=\alpha C+\gamma P_{pub}$, $h=\alpha^{-1}H_2(m,Y')+\beta$,并将 h 发送给签名人。

(c)签名(阶段 2)。签名人计算 $S=(r+h)S_{ID}+rH_1(c)$,并将 S 发送给用户。

(d)解盲。用户计算 $S'=\alpha S$,并输出部分盲签名(Y',C',S',m,c)。

d)签名验证。检查下列等式:

$$e(S',P)=e(Y'+H_2(m,Y')Q_{ID},P_{pub})e(H_1(c),C')$$

是否成立。若成立则接受该签名,否则拒绝该签名。

2)性能评价

Chow 等人证明了 Chow-Hui 方案的部分盲性和不可伪造性。不过由于 Chow 等人在证明 Chow-Hui 方案的不可伪造性时使用的安全模型是不完善的,因此 Chow-Hui 方案的不可伪造性还是有一定疑问的。可以看到,Chow-Hui 方案在签名发布时用户要进行六次群 $\mathbb{G}_1$ 上的点乘运算。一般来说,用户的计算能力比签名人的计算能力要弱得多,因此在 Chow-Hui 方案中用户的计算负担是比较重的。Chow-Hui 方案在签名验证时要进行三次双线性对运算,因此其在效率上还有待进一步提高。

3 无证书部分盲签名研究

3.1 研究现状

2003 年 Al-Riyami 等人[23] 提出了无证书公钥密码体制的思想。无证书公钥密码系统不仅保持了基于身份的密码系统

无须公钥证书的优点,而且由于在无证书公钥密码系统中,密钥生成中心(KGC)只能获得用户的部分私钥而并不能获得用户的完整私钥,因此无证书公钥密码系统消除了基于身份的密码系统固有的密钥托管问题。这样无证书公钥密码系统不仅很好地融合了基于 PKI 的公钥密码系统和基于身份的密码系统的优点,而且在一定程度上克服了它们各自的缺点,因此无证书公钥密码系统是一种性能优良的公钥密码系统。无证书公钥密码学的研究进展可参阅文献[24]。

2008 年荣维坚[25]提出了一个无证书部分盲签名方案。2009年苏万力等人[26]也提出了一个无证书部分盲签名方案。不过荣方案[25]和苏—谭方案[26]都没有严格证明方案的不可伪造性。2009 年 Zhang 等人[27]定义了一个无证书部分盲签名的安全模型,并提出了一个可证安全的无证书部分盲签名方案。但是 Zhang 等人[27]定义的无证书部分盲签名的安全模型存在与 Chow-Hui 基于身份的部分盲签名安全模型同样的问题,它也不能俘获无证书部分盲签名方案遭受的窜改协商信息攻击。下面具体介绍苏—谭无证书部分盲签名方案[26]。

3.2　苏—谭无证书部分盲签名方案

1)方案描述

a)建立。KGC 选择阶为 q 的循环群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$,定义双线性对 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$;任意选择群 $\mathbb{G}_1$ 的生成元 P,随机选择 $s\in\mathbb{Z}_q^*$,计算 $P_{\text{pub}}=sP$;选取三个密码哈希函数 $H_1:\{0,1\}^*\to\mathbb{G}_1$,$H_2:\mathbb{G}_1\to\mathbb{Z}_q^*$,$H_3:\{0,1\}^*\to\mathbb{Z}_q^*$。系统参数为 params = $\{\mathbb{G}_1,\mathbb{G}_2,e,q,P,P_{\text{pub}},H_1,H_2,H_3\}$,主秘密值为 s。

b)部分私钥生成。签名人向 KGC 提交其身份 ID_A,KGC 计算 $Q_A=H_1(\text{ID}_A)$,$D_A=sQ_A$,并将部分私钥 D_A 通过安全信道发送给签名人。

c)签名人秘密值生成。签名人任意选择 $x_A\in\mathbb{Z}_q^*$,并将 x_A 作为其秘密值。

d)签名人公钥产生。签名人设置其公钥为 $PK_A=x_AP$,并令 $R_A=PK_A$。

e)签名人私钥产生。签名人计算 $y_A=H_2(R_A)$,$S_A=\dfrac{1}{x_A+y_A}\times D_A$,设置其私钥为 $SK_A=S_A$。

f)签名发布。假设 c 为事先协商的公共信息,则签名人与用户的交互过程如下:

(a)签名(阶段 1)。签名人随机选择 $r\in\mathbb{Z}_q^*$,计算 $C=rP$,$Y=rQ_A$,并将(Y,C)发送给用户。

(b)盲化。用户随机选择 $\alpha,\beta,\gamma\in\mathbb{Z}_q^*$,计算 $Y'=\alpha Y+\alpha\beta Q_A-\gamma H_1(c)$,$C'=\alpha C+\gamma P_{\text{pub}}$,$h=\alpha^{-1}H_3(m,Y')+\beta$,并将 h 发送给签名人。

(c)签名(阶段 2)。签名人计算 $S=(r+h)S_A+rH_1(c)\times\dfrac{1}{x_A+y_A}$,并将 S 发送给用户。

(d)解盲。用户计算 $S'=\alpha S$,并输出部分盲签名(Y',C',S',m,c)。

g)签名验证。验证者计算 $Q_A=H_1(\text{ID}_A)$,$y_A=H_2(R_A)$,并验证下列等式:

$$e(S',R_A+y_AP)=e(Y'+H_3(m,Y')Q_A,P_{\text{pub}})e(H_1(c),C')$$

是否成立。如果成立,则签名是合法的;否则签名不是合法的。

2)性能评价

无证书公钥密码方案虽然不是纯基于身份的,但它实际上是很接近基于身份的,因此无证书公钥密码方案可在基于身份的密码方案的基础上构造。可以看出,苏—谭无证书部分盲签名方案是在 Chow-Hui 基于身份的部分盲签名方案的基础上设计的,因此在苏—谭方案中用户的计算负担也是比较重的。苏—谭方案在签名验证时要进行四次双线性对运算,因此苏—谭方案的效率也不高。

4　结束语

综上所述,部分盲签名一经提出便引起了人们的密切关注。国内外学者对其进行了深入的研究,并取得了一批有价值的研究成果。虽然如此,在部分盲签名方面仍有以下一些问题有待进一步探讨:

a)因为基于身份的部分盲签名的安全模型和无证书部分盲签名的安全模型都存在安全缺陷,而适当的安全模型是设计安全的密码方案的前提,所以借鉴部分盲签名的安全模型[4]定义基于身份的部分盲签名的安全模型和无证书部分盲签名的安全模型是一个亟待解决的问题。

b)在基于身份的密码体制和无证书公钥密码体制下提出的部分盲签名方案还是很少的,并且这有限的几个方案要么在安全性上存在缺陷,要么在效率上存在不足。基于身份的密码体制和无证书公钥密码体制因其特性而在资源受限的环境中具有重要的应用。因此,设计安全、高效的基于身份的部分盲签名方案和无证书部分盲签名方案是一项重要的研究课题。

c)由于将部分盲签名与群签名、代理签名以及门限签名结合起来对于电子现金等领域具有更大的应用价值,因此设计群部分盲签名、代理部分盲签名以及门限部分盲签名是一个有意义的研究课题。

d)由于在随机预言模型下安全的密码方案在现实环境中不一定是安全的,因此设计在标准模型下安全的密码方案不仅具有重要的理论意义,而且具有重大的应用价值。目前人们还没有提出在标准模型下安全的基于身份的部分盲签名方案与无证书部分盲签名方案,因此设计在标准模型下安全的基于身份的部分盲签名方案和无证书部分盲签名方案是一个急需探索的研究课题。

e)随着公钥密码学的发展,在新型公钥密码体制下,如基于模糊身份的公钥密码体制[28,29]和基于格的公钥密码体制[30,31]等,研究与部分盲签名有关的问题,如安全模型的定义、高效方案的构造等,是一个应予关注的研究课题。

f)因为要解决电子现金的匿名性问题,所以 Chaum[1]提出了盲签名的概念。由此利用已提出的部分盲签名方案设计高效、安全的电子现金、电子投票系统是一个应致力研究的课题。

笔者将继续从事部分盲签名及其应用的研究,并将在后续工作中部分地解决上述问题。可以预见,部分盲签名仍将是信息安全领域的研究热点,并将在电子商务和电子政务等领域扮演越来越重要的角色。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[C]//Proc of CRYPTO 1982. New York: Plenum Press,1983:199-203.

[2] ABE M, FUJISAKI E. How to date blind signatures[C]//Proc of ASIACRYPT 1996. Berlin:Springer-Verlag,1996:244-251.

[3] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Trans on Information Theory,1976,22(6): 644-654.

[4] ABE M, OKAMOTO T. Provably secure partially blind signatures [C]//Proc of CRYPTO 2000. Berlin: Springer-Verlag, 2000: 271-

286.
[5] JUELS A, LUBY M, OSTROVSKY R. Security of blind digital signatures[C]//Proc of CRYPTO 1997. Berlin: Springer-Verlag, 1997: 150-164.
[6] WU Qian-hong, SUSILO W, MU Yi, *et al*. Efficient partially blind signatures with provable security[C]//Proc of International Conference on Computational Science and its Applications. Berlin: Springer-Verlag, 2007: 1096-1105.
[7] CAO Tian-jie, LIN Dong-dai, XUI Rui. A randomized RSA-based partially blind signature scheme for electronic cash[J]. Computers and Security, 2005, 24(1): 44-49.
[8] MARTINET G, POUPARD G, SOLA P. Cryptanalysis of a partially blind signature scheme or how to make $100 bills with $1 and $2 ones[C]//Proc of Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2006: 171-176.
[9] HUANG Hui-feng, CHANG C C. A new design of efficient partially blind signature scheme[J]. Journal of Systems and Software, 2004, 73(3): 397-403.
[10] ZHANG Fang-guo, CHEN Xiao-feng. Cryptanalysis of Huang-Chang partially blind signature scheme[J]. Journal of Systems and Software, 2005, 76(3): 323-325.
[11] ZHANG Fang-guo, SAFAVI-NAINI R, SUSILO W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings [C]//Proc of INDOCRYPT 2003. Berlin: Springer-Verlag, 2003: 191-204.
[12] CHOW S S M, HUI L C K, YIU S M, *et al*. Two improved partially blind signature schemes from bilinear pairings[C]//Proc of the 10th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2005: 316-328.
[13] OKAMOTO T. Efficient blind and partially blind signatures without random oracles[C]//Proc of the 3rd Theory of Cryptography Conference. Berlin: Springer-Verlag, 2006: 80-99.
[14] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYPTO 1984. Berlin: Springer-Verlag, 1984: 47-53.
[15] 曾梦岐, 卿昱, 谭平璋, 等. 基于身份的加密体制研究综述[J]. 计算机应用研究, 2010, 27(1): 27-31.
[16] HU Xiao-ming, HUANG Shang-teng. An efficient ID-based partially blind signature scheme[C]//Proc of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Washington DC: IEEE Computer Society, 2007: 291-296.
[17] TSENG Y M, WU T Y, WU J D. Forgery attacks on an ID-based partially blind signature scheme[EB/OL]. (2008-08-21)[2012-04-19]. http://www.iaeng.org/IJCS/issues_v35/issue_3/IJCS_35_3_07.pdf.
[18] 张学军, 王育民. 高效的基于身份的部分盲签名方案[J]. 计算机工程与应用, 2007, 43(11): 211-213.
[19] 闫东升. 一个新的高效的基于身份的部分盲签名方案[J]. 计算机工程与应用, 2008, 44(2): 137-140.
[20] 崔巍, 辛阳, 胡程瑜, 等. 高效的基于身份的(受限)部分盲签名[J]. 北京邮电大学学报, 2008, 31(4): 53-57.
[21] 李明祥, 赵秀明, 王洪涛. 对一种部分盲签名方案的安全性分析与改进[J]. 计算机应用, 2010, 30(10): 2687-2690.
[22] 李明祥, 郑艳娟, 安文广. 一种高效的基于身份的部分盲签名方案[J]. 计算机应用研究, 2010, 27(11): 4299-4302.
[23] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Proc of the ASIACRYPT 2003. Berlin: Springer-Verlag, 2003: 452-473.
[24] 张福泰, 孙银霞, 张磊, 等. 无证书公钥密码体制研究[J]. 软件学报, 2011, 22(6): 1316-1332.
[25] 荣维坚. 无证书部分盲签名方案[J]. 漳州师范学院学报: 自然科学版, 2008, 62(4): 44-47.
[26] 苏万力, 谭示崇, 李艳平, 等. 无证书部分盲签名[J]. 吉林大学学报: 工学版, 2009, 39(4): 1094-1098.
[27] ZHANG Lei, ZHANG Fu-tai. Certificateless partially blind signatures [C]//Proc of the 1st International Conference on Information Science and Engineering. Washington DC: IEEE Computer Society, 2009: 2883-2886.
[28] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Proc of EUROCRYPT 2005. Berlin: Springer-Verlag, 2005: 457-473.
[29] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, *et al*. Fuzzy identity based encryption from lattices[EB/OL]. (2011-08-01)[2012-04-19]. http://eprint.iacr.org/2011/414.
[30] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai tree, or how to delegate a lattice basis[C]//Proc of EUROCRYPT 2010. Berlin: Springer-Verlag, 2010: 523-552.
[31] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[EB/OL]. (2011-09-14)[2012-04-19]. http://eprint.iacr.org/2011/501.

(上接第 4431 页)

[32] 李明, 苗付友, 熊焰. 一种基于簇的 WSN 预分配密钥管理机制[J]. 计算机工程, 2011, 37(5): 1-4.
[33] 李明, 苗付友, 熊焰. 基于簇的无线传感器网络预分配密钥机制[J]. 计算机工程, 2011, 37(20): 127-132.
[34] PERRIG A, TYGAR J D, SONG D, *et al*. Efficient authentication and signing of multicast streams over lossy channels[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2000: 56-73.
[35] 易叶青, 林亚平, 彭舸, 等. 无线传感器网络中不依赖 MAC 认证的虚假数据过滤算法[J]. 通信学报, 2009, 30(6): 53-63.
[36] 董晓梅, 赵枋, 李晓华, 等. 适用于无线传感器网络的数字水印技术[J]. 武汉大学学报: 理学版, 2009, 55(1): 125-128.
[37] 易叶青, 林亚平, 李小龙, 等. WSN 中基于协作水印的虚假数据过滤算法[J]. 软件学报, 2010, 21(1): 107-118.
[38] YE Fan, YANG Hao, LIU Zhen. Catching "moles" in sensor networks [C]//Proc of the 27th International Conference on Distributed Computing Systems. Washington DC: IEEE Computer Society, 2007: 69-77.
[39] 杨峰. 无线传感器网络恶意节点防范技术[D]. 合肥: 中国科技技术大学, 2009.
[40] 杨峰, 周学海, 张起元, 等. 无线传感器网络恶意节点溯源追踪方法研究[J]. 电子学报, 2009, 37(1): 202-206.
[41] YANG Feng, ZHOU Xue-hai, ZHANG Shu-guang. Hierarchical traceback in wireless sensor networks[C]//Proc of the 4th International Conference on Wireless Communications, Networking and Mobile Computing. 2008: 1-4.
[42] 谢婧, 李曦, 杨峰. 应对虚假数据注入结合途中过滤与溯源追踪方法[J]. 计算机系统应用, 2011, 20(12): 249-256.
[43] 杨峰, 周学海, 张起元. 无线传感器网络高覆盖、低延迟途中过滤方法研究[J]. 计算机工程与科学, 2010, 32(11): 20-24.
[44] 江长勇. 无线传感器网络中的攻击检测研究[D]. 镇江: 江苏大学, 2009.
[45] 孙利民, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005.