软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(6):1316−1332 [doi: 10.3724/SP.J.1001.2011.04007]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无证书公钥密码体制研究*

张福泰[1+], 孙银霞[2], 张 磊[3], 耿曼曼[1], 李素娟[1,4]

[1](南京师范大学 计算机科学与技术学院,江苏省信息安全保密技术工程研究中心,江苏 南京 210097)

[2](西安电子科技大学 教育部计算机网络与信息安全重点实验室,陕西 西安 710071)

[3](UNESCO Chair in Data Privacy, Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Catalonia 43007, Spain)

[4](南京工业大学 理学院,江苏 南京 210009)

Research on Certificateless Public Key Cryptography

ZHANG Fu-Tai[1+], SUN Yin-Xia[2], ZHANG Lei[3], GENG Man-Man[1], LI Su-Juan[1,4]

[1](Jiangsu Engineering Research Center of Information Security and Privacy Protection Technology, School of Computer Science and Technology, Nanjing Normal University, Nanjing 210097, China)

[2](Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)

[3](UNESCO Chair in Data Privacy,Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Catalonia 43007, Spain)

[4](College of Sciences, Nanjing University of Technology, Nanjing 210009, China)

+ Corresponding author: E-mail: zhangfutai@njnu.edu.cn

Zhang FT, Sun YX, Zhang L, Geng MM, Li SJ. Research on certificateless public key cryptography. *Journal of Software*, 2011,22(6):1316−1332. http://www.jos.org.cn/1000-9825/4007.htm

Abstract: Certificateless public key cryptography (CL-PKC for short) is a new type of public key cryptography, which is developed on the foundation of identity based cryptography (ID-PKC for short). CL-PKC elimilates the key escrow problem and the need for public key certificate. These two advantages are what makes it attractive to the research community and industrial world form the beginning of its birth. It has been a very active research hot topic in the field of cryptology and information security. In about seven years, the study of CL-PKC has advanced step by step, making its theories and techniques more and more enriching. This paper revisits, analyzes, compares, and briefly reviews some of the main results. Furthermore, this study discusses some existing problems in this research field that deserve further investigation.

Key words: certificateless public key cryptography; certificateless encryption; certificateless signature; certificateless key agreement

摘 要: 无证书公钥密码体制(certificateless public key cryptography,简称 CL-PKC)是在基于身份的公钥密码体制(identity-based public key cryptography,简称 ID-PKC)的基础上提出来的一种新型公钥密码体制,没有密钥托管问题、

* 基金项目: 国家自然科学基金(60673070); 江苏省自然科学基金(BK2006217); 南京工业大学青年教师学术基金(39704023)
收稿时间: 2010-05-20; 定稿时间: 2011-02-15
CNKI 网络优先出版: 2011-03-24 15:03, http://www.cnki.net/kcms/detail/11.2560.TP.20110324.1503.001.html

不需要使用公钥证书,使得无证书公钥密码体制从其概念提出的初始就受到了学术界和工业界的极大关注.从2003年至今,它一直是密码学和信息安全领域非常活跃的研究热点.其理论和技术在不断地丰富和发展.到目前为止,已经积累了大量的研究成果.将对这些成果进行较为系统的整理、分析、比较和简要的评述,并探讨该领域研究尚存在的不足及值得进一步研究的问题.

关键词: 无证书公钥密码体制;无证书加密;无证书签名;无证书密钥协商;安全模型

中图法分类号: TP309 **文献标识码:** A

Diffie 和 Hellman[1]于 1976 年提出的公钥密码学(public key cryptography,简称 PKC)的概念引起了密码学历史上的一次巨大变革,开创了密码学和网络信息安全发展的新纪元.公钥密码学能够很好地解决经典的对称密码体制所固有的密钥管理困难以及不能为不可否认性(non-repudiation)提供理想的解决方法等问题,不仅使对称密码体制的使用更加方便和可靠,而且使密码学在网络和信息安全中发挥的作用更加广泛和突出.公钥加密和密钥协商为密钥管理提供了有效的技术途径.数字签名(digital signature)理论与技术的发展,为信息安全中的不可否认性需求的满足给出了切实有效的解决方法,极大地促进了电子商务、电子政务以及各种管理系统的数字化进程.目前,公钥密码理论与技术的发展正在为各种各样的信息系统的安全性发挥着不可或缺的保障作用.

在公钥密码系统中,每个用户拥有一对相匹配的公私钥.其中的公钥对外公开,私钥由用户自己安全保管.用户 Bob 用 Alice 的公钥来加密要发送给 Alice 的机密信息或验证 Alice 的签名;Alice 用自己的私钥来解密其他用户发来的密文或者产生自己对一些消息的签名.当传统公钥密码系统用来实现保密和认证功能时,必须解决好一个基本问题,那就是如何保证用户公钥的真实性和有效性.传统的解决方法是使用公钥基础设施 PKI (public key infrastructure).PKI 的核心组成部分是证书中心 CA(certificate authority).CA 负责为用户签发公钥证书(public key certificate),用以保证系统中用户公钥的真实性和有效性.证书中通常包含用户的身份信息、公钥和其他必要的信息,如所使用的加密和签名算法、证书的有效期等.CA 维护着一个动态变化的证书库(或叫证书目录),该证书库向网络中的所有用户开放.一个用户在和 Alice 通信之前,先在证书库中查找 Alice 的公钥证书,获得 Alice 的公开密钥,这样就可以和 Alice 进行保密通信了.当 Bob 把自己对某个消息的签名发给网络中另一用户时,需要在签名后附上自己的公钥证书,接收者收到后,先验证 Bob 的公钥证书的有效性,再用 Bob 的公钥验证签名.公钥证书较好地解决了公钥的真实性和有效性问题,使得 PKI 能够为网络用户提供较好的安全服务.但公钥证书库的管理和维护需要巨大的计算、通信和存储代价.

1984 年,Shamir 提出了基于身份的密码系统(identity-based cryptography)[2],他以另外一种方式解决了公钥的真实性问题,避免了基于 PKI 的传统公钥密码系统中对证书的使用和验证过程.在基于身份的密码系统中,用户的公钥是一些公开的、可以唯一确定用户身份的信息,一般这些信息称为用户的身份(ID).在实际应用中,用户的身份可以是姓名+通信地址、手机号码、身份证号码或 E-Mail 地址等.在使用基于身份的密码系统进行保密和认证时,由于我们已经知道对方的公开身份信息,所以就不需要在数据库中查找用户的公钥,也不需要对公钥的真实性进行检验.因此,基于身份的密码系统无须公钥证书的存在.在基于身份的系统中,所有用户的私钥都是由一个可信的第三方——私钥生成中心 PKG(private key generation center)利用它掌握的系统唯一的主密钥(master key)产生的.因此,这样的系统中不可避免地存在一个固有的缺陷,即私钥托管问题.PKG 知道任何用户的私钥,因而不诚实的 PKG 可以窃听任何用户的通信,并可以伪造任何用户的签名.一些学者对如何化解基于身份的系统因私钥托管所带来的弊端做了一些探索,但无法从根本上解决问题.

无证书公钥密码系统(certificateless public key cryptography)[3]正是为了克服基于身份的系统中的私钥托管(key escrow)问题而提出的,其概念由 Al-Riyami 和 Paterson[3]于 2003 年提出.与基于 PKI 的传统公钥密码系统相比,无证书的公钥密码系统和基于身份的系统一样不需要公钥证书,同时,无证书密码系统消除了基于身份的系统中的私钥托管问题.可以说,无证书公钥密码系统不仅很好地结合了上述两种密码系统的优点,而且从一定程度上克服了它们的缺点,是一种性能优良、便于应用的公钥密码系统.

在无证书的公钥密码系统中,仍然存在一个可信的第三方密钥生成中心 KGC(key generation center),它拥有系统的主密钥(master key).KGC 的作用是根据用户的身份和系统主密钥计算用户的部分私钥,并安全地传送给用户.在安全地收到自己的部分私钥后,用户再使用自己的部分私钥和自己随机选择的一个秘密值生成自己完整的私钥,公钥由自己的秘密值、身份和系统参数计算得出,并以可靠的方式公布.之后,就可以用自己的私钥进行解密和签名.在这样的系统中,KGC 无法得知任何用户的私钥.从而,无证书密码体制有效克服了基于身份系统中的私钥托管问题.近年来,无证书密码体制引起了学术界的极大关注,一直是密码学与信息安全领域突出的研究热点之一.有不少学术团体和科研机构在对这一新的密码系统进行探索研究,相继取得了有意义的研究成果.本文将从无证书加密、无证书签名、无证书密钥协商等几方面对这一研究领域的现状及主要成果进行概括和分析,并探讨该领域研究尚存在的不足和值得进一步研究的问题.

1 无证书加密

本节讨论无证书加密的定义、安全性概念,然后对现有的无证书加密方案进行总结、分析,最后指出在无证书加密方面需要进一步研究的一些问题.

1.1 无证书加密方案的基本概念

无证书加密主要有 3 种定义模式:Al-Riyami 和 Paterson 定义(简称 AP 定义)、简化定义、Baek,Safavi-Naini 和 Susilo 定义(简称 BSS 定义).

1.1.1 AP 定义

Al-Riyami 和 Paterson 在文献[3]给出的无证书加密方案的定义,称为 AP 定义,其描述如下:

一个无证书加密方案由以下 7 个概率多项式时间算法构成:

(1) 系统设置算法 Setup:输入安全参数 1^k,输出系统私钥 *msk* 和系统公开参数 *params*;

(2) 提取部分私钥算法 Extract-Partial-Private-Key:输入 *params*,*msk* 和用户身份 *ID*,输出该用户的部分私钥 d_{ID}.该算法由 KGC 运行,并通过安全信道把 d_{ID} 发送给用户;

(3) 设置秘密值算法 Set-Secret-Value:输入 *params* 和用户身份 *ID*,输出用户 *ID* 的秘密值 x_{ID};

(4) 设置私钥算法 Set-Private-Key:输入 *params*、用户 *ID* 的部分私钥 d_{ID} 和秘密值 x_{ID},输出用户 *ID* 的私钥 sk_{ID};

(5) 设置公钥算法 Set-Public-Key:输入 *params* 和用户 *ID* 的秘密值 x_{ID},输出该用户的公钥 pk_{ID};

(6) 加密算法 Encrypt:输入 *params*、接收方身份 *ID*、公钥 pk_{ID} 和消息 *M*,输出密文 *C* 或者错误标识⊥;

(7) 解密算法 Decrypt:输入 *params*、接收方身份 *ID*、私钥 sk_{ID} 和密文 *C*,输出消息 *M* 或者错误标识⊥.

1.1.2 简化定义

可以把 AP 定义中的设置秘密值算法和设置公钥算法合并为一个用户密钥设置算法 Set-User-Key.文献[4]进一步省略了设置私钥算法.在简化的无证书加密方案的定义中,一个无证书加密方案由以下 5 个概率多项式时间算法构成:

(1) Setup:同 AP 定义;

(2) Extract-Partial-Private-Key:同 AP 定义;

(3) Set-User-Key:输入 *params* 和用户身份 *ID*,输出其秘密值 x_{ID} 和公钥 pk_{ID};

(4) Encrypt:同 AP 定义;

(5) Decrypt:输入 *params*、接收方身份 *ID*、部分私钥 d_{ID}、秘密值 x_{ID} 和密文 *C*,输出消息 *M* 或者错误标识⊥.

该定义与 AP 定义在功能上是一样的,但是对安全模型有影响.基于 AP 定义的安全模型,允许攻击者询问部分私钥和私钥,但是不能询问秘密值;而基于该简化定义的安全模型,攻击者能够询问秘密值[4,5],所以攻击者变得更加强大.

1.1.3 BSS 定义

与以上定义有所区别的一个无证书加密方案的定义由 Baek,Safavi-Naini 和 Susilo 提出[6].在该定义模式下,完整的用户公钥只有在用户从 KGC 获取部分私钥后才可以计算.BSS 定义由 7 个概率多项式时间算法组成,其中,提取部分密钥算法 Extract-Partial-Key 和设置公钥算法 Set-Public-Key 不同于 AP 定义.

- Extract-Partial-Key:输入 *params*,*msk* 和用户身份 *ID*,输出该用户的部分私钥 d_{ID} 和部分公钥 w_{ID}.该算法由 KGC 运行,并通过安全信道把 d_{ID} 传输给用户,而 w_{ID} 可在公开信道上传输;
- Set-Public-Key:输入 *params*、用户 *ID* 的部分公钥 w_{ID} 和秘密值 x_{ID},输出该用户的公钥 pk_{ID}.

1.2 安全模型

对无证书加密方案的安全性,我们主要针对被广泛接受和使用的 AP 定义模式和适应性选择密文攻击[7]来讨论.

无证书体制下用户密钥的产生方式决定了两类攻击者,分别称为第 1 类攻击者和第 2 类攻击者.其中:第 1 类攻击者模拟外部攻击者,能够替换任何用户的公钥;第 2 类攻击者模拟诚实但好奇的 KGC.

IND-CCA2 安全性:对一个无证书加密方案来说,如果攻击者 A 在以下与挑战者 Challenger 的游戏中不能以不可忽略的优势获胜,那么我们说该方案在适应性选择密文攻击下,密文是不可区分的,即具有 IND-CCA2 安全性[3−6].

游戏:

(1) $(params,msk)\leftarrow Challenger^{Setup}(1^k)$,

(2) $(ID^*,(M_0,M_1))\leftarrow A^{oracles}(params,inf)$,

(3) $b\leftarrow\{0,1\}$, $C^*\leftarrow Challenger^{Encrypt}(M_b,ID^*)$,

(4) $b'\leftarrow A^{oracles}(params,inf,C^*)$.

A 获胜,当且仅当 $b'=b$.

我们定义攻击者在以上游戏中的优势为 $2|\Pr[b'=b]-1/2|$.如果 A 为第 1 类攻击者,那么 $inf=\varnothing$;如果 A 为第 2 类攻击者,那么 $inf=msk$.攻击者在游戏的阶段(2)和阶段(4)可访问如下的预言器(oracles):

- 部分私钥询问(第 1 类攻击者):攻击者提供一个用户身份 *ID*,挑战者运行提取部分私钥算法得到该用户的部分私钥 d_{ID},并把 d_{ID} 返回给攻击者;
- 私钥询问:攻击者提供一个用户身份 *ID*,挑战者运行算法 Set-Private-Key 得到该用户的私钥 sk_{ID},并把 sk_{ID} 返回给攻击者;
- 公钥询问:攻击者提供一个用户身份 *ID*,挑战者运行算法 Set-Public-Key 得到该用户的公钥 pk_{ID},并把 pk_{ID} 返回给攻击者;
- 公钥替换:攻击者可以替换任何用户的公钥;
- 解密询问:解密预言器分为 3 类:
  - 强解密:攻击者提供身份 *ID* 和密文 *C*,挑战者用该用户当前公钥(无论是否被替换)对应的私钥解密 *C*,然后把解密结果返回给攻击者;
  - 弱解密:攻击者提供身份 *ID*、秘密值 x_{ID} 和密文 *C*,挑战者通过部分私钥和秘密值计算出 *ID* 的完整私钥,然后用该私钥解密 *C*,并把解密结果返回给攻击者;
  - 一般解密:攻击者提供身份 *ID* 和密文 *C*,挑战者用该用户原来的私钥解密 *C*,然后把解密结果返回给攻击者.

在以上游戏中,攻击者会因所拥有的资源和能力的不同而受不同条件的约束,这些约束包括:

(1) 在任何时候都不能询问挑战身份 ID^*的私钥;

(2) 如果某个公钥已被替换,那么不能询问该公钥对应的私钥;

(3) 对于第 1 类攻击者,如果用来生成挑战密文 C^*的公钥是攻击者替换后的公钥,那么任何时候都不能询问挑战身份 ID^*的部分私钥;

(4) 对于第 2 类攻击者,不允许替换挑战身份 ID^*的公钥.

根据解密预言器的强弱,Dent[5]把第 1 类攻击者分为 3 种:强一类攻击者,弱一 a 类攻击者,弱一 b 类攻击者和弱一 c 类攻击者(按其定义,弱一 c 类攻击者不允许替换公钥,这与实际情况不符,所以本文不考虑此类攻击者):

- 强一类攻击者:能够询问强解密预言器,但不能询问 C^*在 ID^*下的解密,除非公钥被替换;不能询问弱解密和一般解密预言器;
- 弱一 a 类攻击者:任何时候不能询问强解密预言器;能够询问弱解密预言器和一般解密预言器,但不能询问 C^*在 ID^*下的解密,除非公钥被替换;
- 弱一 b 类攻击者:既不能询问强解密预言器,也不能询问弱解密预言器;只能询问一般解密预言器,但不能询问 C^*在 ID^*下的解密,除非用来生成 C^*的公钥不是 ID^*原来的公钥.

根据是否可以替换公钥以及解密预言器的强弱,Dent[5]把第 2 类攻击者分为两类:强二类攻击者和弱二类攻击者:

- 强二类攻击者:可以替换公钥;能够询问强解密预言器,但是不能询问挑战密文 C^*在挑战身份 ID^*下的解密,除非公钥被替换;既不能询问弱解密预言器,也不能询问一般解密预言器;
- 弱二类攻击者:任何时候不能替换用户公钥;能询问一般解密预言器,但不能询问 C^*在 ID^*下的解密;既不能询问强解密预言器,也不能询问弱解密预言器.

1.3 无证书加密方案

近几年,对无证书加密的研究已经取得很多成果,各种各样的无证书加密方案相继出现.

第 1 个无证书加密方案[3]在随机预言模型(ROM)[8]下被证明是安全的,但其加解密涉及的双线性对运算较多、效率较低.两年后,他们构造了一个高效的方案[9],但不久被 Libert-Quisquater[10]以及 Zhang-Feng[11]攻破并改进.其中,Zhang-Feng 的方案类似于 Cheng-Comley 的方案[4],后者在 ROM 下只给出了弱安全性证明.Shi-Li 通过另一种部分私钥生成方式构造了一个无证书加密方案[12],他们的方案与 Libert-Quisquater 方案[10]相似.早期的无证书加密方案都是基于双线性映射的,由于双线性映射的计算代价相对于模指数运算要高出很多,所以这些方案的实现效率在一定程度上都受到了限制.针对这一问题,Baek 等人在文献[6]中提出了第 1 个不使用双线性对的无证书加密方案.该方案运行效率高,但其安全性证明存在缺陷[13].文献[13,14]在文献[6]中方案的基础上,分别提出了不使用双线性对的无证书加密方案.文献[13]中的方案是可证明安全的,但与文献[6]相比增加了一些计算量.我们指出,文献[14]中第 1 个方案存在与文献[6]中方案相同的安全性证明缺陷,即无法把第 1 类安全性归结于计算 Diffie-Hellman 问题(即文献[14]中 Theorem 1 不成立).文献[14]中第 2 个方案是抗“拒绝解密攻击(denial-of-decryption)”[15]的.随后,Wang 等人[16]对满足第 3 安全等级的无证书加密方案重新定义了安全模型,并指出了文献[14]中第 2 个方案在新安全模型下是不安全的:攻击者在获得挑战用户的秘密值和挑战密文后,替换挑战用户的公钥,并询问挑战用户在替换后的公钥下的部分密钥 PSK'_{ID},最后根据 PSK'_{ID} 计算出挑战身份原来的部分密钥 PSK_{ID},从而获得挑战身份的完整私钥.然而我们指出,上述攻击是不成立的:虽然 PSK_{ID} 确实是一个有效的与挑战身份对应的部分密钥,但是不一定就是挑战者用来生成挑战密文的密钥(“是”的概率仅为 $1/(q-1)$),因为 w 是由挑战者任意选取的,而不是由攻击者决定的.文献[17]提出了通信代价更低的无证书加密方案.Lai 等人[18]基于 RSA 假设提出了一个更为高效的无证书加密方案,首次把无证书加密建立在大整数因子分解困难问题之上,其不足是安全模型较弱.Selvi 等人在文献[19]中提出了基于 RSA 的 CCA2 安全的无证书加密方案.文献[20]中,Lee 等人讨论了无证书认证加密问题.Ju 等人在文献[21]中探讨了无证书体制下的公钥撤销问题,但其解决方法还有待改进.

上述方案的安全性都是在随机预言模型下证明的.Liu 等人[15]首次在标准模型(STM)下构造了无证书加密方案,但是安全性较弱;随后,Park 等人[22]和 Dent 等人[23]分别在标准模型下给出了可证明安全的无证书加密方案.

Au 等人[24]考虑了恶意 KGC 攻击,即一个恶意的 KGC 在设置系统参数时加入额外的限门信息,以便其推导

出用户的完整私钥.Hwang 等人[25]在标准模型下考虑了抗恶意 KGC 攻击的无证书加密方案的构造.

以上讨论的都是具体方案,对于无证书加密的一般构造方法的研究也有不少成果.所谓一般构造方法是指用已有的其他密码原型来构造无证书加密的方法.直观地,可以把基于身份的加密和传统公钥加密结合起来构造无证书加密.首先给出无证书加密的一般构造方法的是 Al-Riyami[26]和 Yum-Lee[27],但是这两种构造方法都是不安全的[10,28].Bentahar 等人[29,30]用密钥封装/数据封装机制构造了无证书加密.建立在基于身份的加密基础上的一般性构造包括文献[10,31].Dent[5]给出了一个基于多重加密的一般性构造方法.此外,在标准模型下,也有一些关于无证书加密的一般构造,如文献[30,32−35].其中,文献[33]的方案可抵抗恶意但被动的 KGC 攻击,文献[30,34,35]中是针对密钥封装讨论的.

文献[5]对已有的一些无证书加密方案和安全模型作了比较和分析.在此基础上,我们进行扩充,主要从密钥长度、计算效率和密文长度等方面对更多的具体方案作总结和比较,见表 1.“模型”栏阐述可证明安全性,例如,“强一、弱二 ROM”是指方案在随机预言模型下对强一类攻击者和弱二类攻击者是 IND-CCA2 可证明安全的.其他类推.IND-CPA 指选择明文安全[18].p:双线性对;s:点乘运算;e:指数运算;$|G_1|$:G_1 中元素的长度;$|G_2|$:G_2 中元素的长度;$|q|$:Zq 中元素的长度;$|g|$:Zp 中元素的长度(p,q 为素数且 $q|p-1$);$|M|$:消息 M 的长度;$|n|$:RSA 模 n 的长度;ROM:随机预言模型;STM:标准模型.

Table 1 Comparison of certificateless encryption schemes

表 1 无证书加密方案比较

Scheme	Key length		Computational cost		Ciphertext length	Security model	Attack
	Secret key	Public key	Encrytpion	Decryption			
Ref.[3]	$\|G_1\|$	$\|G_1\|$	$3p+1s+1e$	$1p+1s$	$\|G_1\|+2\|M\|$	Strong I, weak II, ROM	
Ref.[6]	$2\|q\|$	$2\|g\|$	$4e$	$3e$	$\|g\|+2\|M\|$	Strong I, weak II, ROM	Ref.[13]
Ref.[4]	$\|q\|+\|G_1\|$	$\|G_1\|$	$1p+2s+1e$	$1p+2s$	$\|G_1\|+2\|M\|$	Weak Ib, weak II, ROM	
Ref.[23]	$2\|G_1\|$	$2\|G_1\|$	$1p+3s+1e$	$4p$	$3\|G_1\|+\|M\|$	Strong I, Strong II, STM	
Ref.[10]	$\|q\|+\|G_1\|$	$\|G_2\|$	$1s+2e$	$1p+1s+1e$	$\|G_1\|+2\|M\|$	Strong I, weak II, ROM	
Ref.[15]	$\|q\|+2\|G_1\|$	$2\|G_1\|$	$1p+4s$	$3p+1e$	$3\|G_1\|+2\|M\|$	Weak Ia, weak II, STM	Ref.[31]
Ref.[12]	$\|q\|+\|G_1\|$	$\|G_1\|$	$3s+1e$	$1p+3s$	$\|G_1\|+2\|M\|$	Strong I, weak II, ROM	
Ref.[13]	$2\|q\|$	$3\|g\|+\|q\|$	$6e$	$3e$	$\|g\|+2\|M\|$	Strong I, weak II, ROM	
Ref.[11]	$\|q\|+\|G_1\|$	$\|G_1\|$	$1p+2s+1e$	$1p+2s$	$\|G_1\|+2\|M\|$	No proof	
Ref.[14]-1	$2\|q\|$	$2\|g\|$	$3e$	$2e$	$\|g\|+2\|M\|$	Strong I, weak II, ROM	This paper
Ref.[14]-2	$\|q\|$	$3\|g\|+\|q\|$	$5e$	$2e$	$\|g\|+2\|M\|$	Strong I, weak II, ROM	Ref.[16]
Ref.[16]	$\|q\|$	$3\|g\|+\|q\|$	$5e$	$2e$	$\|g\|+2\|M\|$	Strong I, weak II, ROM	This paper
Ref.[18]	$\|n\|$	$\|n\|$	$3e$	$1e$	$\|n\|+\|M\|$	IND-CPA, ROM	
Ref.[22]	$2\|q\|+\|G_1\|$	$2\|G_1\|$	$4p+5s+2e$	$4p+5s$	$3\|G_1\|+2\|G_2\|+\|Sign\|$	Strong I, weak II, STM	
Ref.[25]	$\|G_2\|+\|Sign\|$	$2\|G_1\|$	$3s+1e+$Verify	$4p$	$3\|G_1\|+\|G_2\|$	Weak Ia, weak II, STM	
Ref.[31]-1	$\|q\|+\|G_1\|$	$\|G_1\|$	$1p+2s+1e$	$1p+2s$	$\|G_1\|+2\|M\|$	Strong I, strong II, ROM	
Ref.[31]-2	$\|q\|+\|G_1\|$	$\|G_1\|$	$4s+1e$	$2p+2s+1e$	$\|q\|+2\|G_1\|+\|M\|$	Strong I, strong II, ROM	

从表 1 可以看出,在随机预言模型下,文献[10,12]中方案的性能较好,其加解密效率较高,且密钥和密文长度适中.在标准模型下,Dent 等人[20]构造的无证书加密方案的性能较好,与另外几个方案[15,22,25]相比,它的密钥和密文更短、计算效率更高.

1.4 需要进一步研究的问题

到目前为止,对于无证书加密,我们认为仍有下列几个值得进一步研究的问题:

(1) 如何构造高效的可证明安全(IND-CCA2)的无双线性对的无证书加密方案?

文献[6]中的方案和文献[14]中的第 1 个方案虽然效率较高,但是安全性证明存在缺陷;而文献[13]中的方案和文献[14]中的第 2 个方案虽然安全性高,但是公钥较长,相当于包含了公钥证书,且用户在做加密之前需要先验证公钥的有效性.可见,其原理与传统的基于公钥证书的系统十分相似.所以实际应用中人们会更倾向于技术较成熟的传统公钥系统;

(2) 如何构造面向任意长度消息(尤其是短消息)的短密文无证书加密方案?

密钥封装机制(key encapsulation mechanism,简称 KEM)与数据封装机制(data encapsulation mechanism,简

称 DEM)组成的混合加密被广泛应用于实际中,KEM 利用公钥技术封装一个对称密钥,DEM 利用对称技术加密一个任意长度消息.在无证书体制下,对混合加密也有一些研究成果[29,30,34].通常的 KEM/DEM 结构要求被加密的消息长度至少为 DEM 的一个分组的长度(一般为 128bit),才能生成最短长度的密文(|随机数|+|消息|).然而,实际中往往需要对很短长度的消息(比如一个 PIN 仅含 4 个数字)进行加密,并且对密文长度也有十分苛刻的要求.这种情况下,常规的 KEM/DEM 混合加密是不适合的.Abe 等人[36]在传统公钥系统下较好地解决了这一问题.但是到目前为止,在无证书体制下还没有有效的解决方案;

(3) 如何构造高效的无证书广播加密和多接收者无证书加密方案?

在无证书系统下,当一个用户给多个用户发送一个消息 M 时,一种直截了当的方法是对每个接收者分别加密消息 M 并发送.这样做的效率显然不高,通信开销较大.然而多接收者保密通信的实际应用非常广泛,如数字电视、视频点播、网络信息服务等.因此,有必要考虑在无证书体制下如何设计高效的广播加密和多个接收者加密方案.

2 无证书签名

2.1 无证书签名方案的基本概念

相对于传统公钥体制和基于身份的公钥体制下的数字签名而言,无证书签名[3,37−58]的优势在于:其一,签名验证者在验证签名时无须像在传统公钥密码系统下那样验证签名者公钥的有效性;其二,没有基于身份的密码系统中的密钥托管问题.

一个无证书签名方案[3,37]由系统参数生成、部分密钥生成、设置秘密值、设置私钥、设置公钥、签名及验证 7 个算法组成.通常,前两个算法由 KGC 执行,而其他算法由签名或验证用户执行.以下是各个算法的描述:

- 系统参数生成:输入安全参数 k,输出系统主密钥 *master-key* 和系统公开参数 *params*.其中,系统公开参数 *params* 向系统中的全体用户公开,而主密钥 *master-key* 则由 KGC 秘密保存;
- 部分密钥生成:输入系统参数 *params*、一个用户的身份 *ID* 和系统主密钥 *master-key*,KGC 为用户输出部分私钥 D_{ID};
- 设置秘密值:输入系统参数 *params* 和用户身份 *ID*,输出该用户的秘密值 x_{ID};
- 设置私钥:输入系统参数 *params*、一个用户的身份 *ID*、该用户的秘密值 x_{ID} 和部分私钥 D_{ID},输出该用户的私钥 S_{ID};
- 设置公钥:输入系统参数 *params*、一个用户的身份 *ID*、秘密值 x_{ID} 和部分私钥 D_{ID},输出该用户的公钥 P_{ID};
- 签名:输入系统参数 *params*、消息 M、一个用户的身份 *ID*、其公钥 P_{ID} 及私钥 S_{ID},输出该用户对消息 M 的签名 σ;
- 验证:输入系统参数 *params*、一个消息 M、一个签名 σ、签名者的身份 *ID* 及公钥 P_{ID},当检验签名有效时,输出 1;否则,输出 0.

2.2 无证书签名的安全模型

与无证书加密系统类似,在无证书签名系统中也有两类攻击者,即第 1 类攻击者 A_{I} 与第 2 类攻击者 A_{II}.第 1 类攻击者不知道系统主密钥,但是可以任意替换用户的公钥;第 2 类攻击者知道系统的主密钥,但是不能替换目标用户的公钥.

最早的无证书签名方案的安全模型由 Huang 等人[37]提出.该模型要求:如果第 1 类攻击者替换了用户 ID 的公钥,那么其在请求 ID 的签名时需要提供 ID 的当前公钥对应的秘密值.这一要求有一定的局限性,一个典型的例子就是 Yap 等人的签名方案[38].该方案在文献[37]中的模型下被证明是安全的,但事实上,对它的各种各样的公钥替换攻击陆续被提出[39−41].在文献[42]中,Zhang 等人给出了一种改进的安全模型,即挑战者回答攻击者的签名请求无须攻击者提供签名者的新公钥对应的秘密值.在文献[43]中,Huang 等人进一步探讨了无证书签名的

安全模型.他们把无证书签名系统中的(第 1 类/第 2 类)攻击者按攻击者的能力从弱到强分成了 3 类:普通、强和超级攻击者.一个普通攻击者只可以得到一些在目标签名者原始公钥下有效的消息-签名对.而对于一个强攻击者,若其在替换用户公钥时能够提供该公钥相对应的秘密值,则就可以得到在替换后的公钥下有效的消息-签名对.最后,对于超级攻击者,即使其在替换用户公钥时不提供该公钥对应的秘密值,也能得到在替换后的公私钥下有效的消息-签名对.

无证书签名方案的安全模型可用下面的挑战者 C 和攻击者 A_{I} 或 A_{II} 间的两个游戏来刻画[43]:

游戏 1(适用于第 1 类攻击者):

初始化:C 运行系统参数生成算法,输入安全参数 k,输出系统主密钥 *master-key* 和系统参数 *params*.C 将 *params* 发送给 A_{I},而对主密钥 *master-key* 严格保密.

攻击:A_{I} 可以适应性地进行公钥询问,部分私钥询问,秘密值询问,公钥替换询问以及签名询问,C 模拟签名方案中的相应算法分别做出回答.其中,根据攻击者能力的强弱,签名预言器可以分为 3 类:

(1) 普通签名预言器:攻击者提供身份 *ID* 和消息 *M*,挑战者用该用户原来的私钥生成 *ID* 对消息 *M* 的签名,然后把签名返回给攻击者;

(2) 强签名预言器:攻击者提供身份 *ID*、秘密值 x_{ID} 和消息 *M*,挑战者通过部分私钥和秘密值计算出 *ID* 的完整私钥,然后用该私钥对 *M* 签名,并把签名结果返回给攻击者;

(3) 超级签名预言器:攻击者提供身份 *ID* 和消息 *M*,挑战者用该用户当前公钥(无论是否被替换)对应的私钥对 *M* 签名,然后把签名结果返回给攻击者.

其中,普通、强和超级攻击者分别可以询问普通签名预言器、强签名预言机和超级签名预言器.

伪造:最后,A_{I} 输出一个四元组(M^*,σ^*,ID^*,P^*).我们说 A_{I} 在游戏中获胜,当且仅当:

(1) σ^*是公钥为 P^*、身份为 ID^*的用户对消息 M^*的一个有效签名;

(2) A_{I} 没有询问过身份为 ID^*的用户的部分私钥;

(3) A_{I} 没有询问过身份为 ID^*、公钥为 P^*的用户对 M^*的签名.

游戏 2(适用于第 2 类攻击者):

初始化:C 运行系统参数生成算法,输出系统主密钥 *master-key* 和系统参数 *params*.C 将 *master-key* 和 *params* 发送给 A_{II}.

攻击:A_{II} 可以适应性地进行公钥询问、秘密值询问、公钥替换询问以及签名询问,C 模拟签名方案中的相应算法分别做出回答.与游戏 1 相同,根据攻击者能力的强弱,签名预言器可分为 3 类.

伪造:最后,A_{II} 输出一个四元组(M^*,σ^*,ID^*,P^*).我们说 A_{II} 在该游戏中获胜,当且仅当:

(1) σ^*是公钥为 P^*、身份为 ID^*的用户对消息 M^*的一个有效签名;

(2) A_{II} 没有询问过身份为 ID^*的用户的秘密值,且 A_{II} 没有替换用户 ID^*的公钥;

(3) A_{II} 没有询问过身份为 ID^*、公钥为 P^*的用户对 M^*的签名.

定义. 一个无证书签名方案在适应性选择消息攻击下,对于普通、强或超级攻击者是存在不可伪造的,当且仅当,任何计算能力多项式受限的普通、强或超级攻击者在以上两个游戏中获胜的概率是可以忽略的.在下文中,我们说一个签名方案是安全的,即指它在适应性选择消息攻击下是存在不可伪造的.

2.3 无证书签名方案

到目前为止,已有大量的无证书签名方案[37−60]被提出.以下根据方案达到的安全级别分类论述.

2.3.1 无安全性证明的方案

第 1 个无证书签名方案由 Al-Riyami 和 Paterson[3]提出,然而作者没有对该方案进行形式化的安全性分析.在文献[37]中,Huang 等人指出了该方案存在的安全缺陷,即它不能抵抗公钥替换攻击.此后,Gorantla 和 Saxena[44]给出了比文献[3]中方案更高效的方案.同样,由于没有形式化的安全性分析,其方案已被 Cao 等人[45]攻破.此外, Harn 等人[46]提出了一个无 Pairing 的无证书签名方案,称该方案安全性基于离散对数问题难解性,但并没有给出严格的形式化安全性证明.文献[58]给出了对两个安全性证明存在较大漏洞的无证书签名方案的

攻击.

2.3.2 安全性证明基于 Huang 等人的模型[37]的方案

在文献[37]中,Huang 等人首次形式化定义了无证书签名的安全模型,并给出了一个在该模型下可证明安全的方案.然而此方案中有大量的 Pairing 计算,导致该方案效率受到很大影响.在文献[38]中,Yap 等人给出了一个较高效的方案,该方案在签名阶段无须 Pairing 计算,而在验证阶段只需两个 Pairing 计算.然而,文献[37]中的模型没有完全捕获第 1 类攻击者的能力.文献[38]的方案虽然有形式化的证明,但实际应用中却是不安全的,文献[39−41]已经给出了多种攻击.到目前为止,在该模型下可证明安全的最高效的方案为 Choi 等人[47]的方案,该方案在签名阶段无需 Pairing 计算而签名验证只需 1 个 Pairing 计算.虽然此方案相当高效,但其签名长度较长.此外,在文献[48]中,Yuan 等人称给出了一个在标准模型下可证明安全的无证书签名方案,然而他们的证明选择了文献[37]中的模型,所以该方案的真正安全性还有待进一步分析.此外,文献[57]研究了在标准模型下具有一定前向安全性的无证书签名,并称该方案在 Huang 等人的模型下得到证明,然而其证明并不严谨.最近,He 等人在文献[60]中给出了一个不使用 Priring 的无证书签名方案,并在 Huang 等人的模型下给出了安全性证明.

2.3.3 对普通攻击者安全的方案

在针对普通攻击者的安全模型(主要指第 1 类攻击者为普通攻击者)下可证明安全的方案主要是几个无证书短签名方案.第 1 个无证书短签名方案由 Huang 等人[43]提出,验证需要 3 个 pairing 计算.Shim[49]对该方案提出了一种攻击,其实,在攻击中对第 1 类攻击者进行了强化,第 1 类攻击者已经成为强或超级攻击者.Du 等人[50]的短签名方案,验证只需计算一个 Pairing.他们称该方案是可证明安全的,然而文献[51]指出了其证明中存在的问题.Tso 等人的无证书短签名方案[52]验证只需计算两个 Pairing,但其公钥较长.

2.3.4 对强攻击者(主要指第 2 类攻击者)安全的方案

被证明对强攻击者安全的无证书签名方案主要出现在文献[42,53]中.文献[42]的方案验证需计算 4 个 Pairing,效率不是很高;文献[53]方案验证只需计算一个 Pairing,但公钥及签名长度较长.在这两个方案的安全性证明中,是把第 2 类攻击者作为强攻击者对待的.但实际上,把第 2 类攻击者看成超级攻击者时,证明也能成立.此外,文献[15]提出了首个具体的在标准模型下可证明安全的无证书签名方案.然而,该方案的安全性基于一个强的假设,并且运行效率较低.

2.3.5 对超级攻击者安全的方案

文献[43,54−56]给出了对超级攻击者安全的无证书签名方案,其中:Hu 等人[54]给出的为一般性构造方法;Huang 等人[43]的方案在一般情况下验证需计算两个 Pairing,且签名长度较长;Zhang 等人[55]的方案与 Huang 等人的方案相比签名长度较短,且在一般情况下计算效率略高于 Huang 等人的方案;文献[56]中的方案在预计算情况下效率高于前两方案,且签名长度和文献[55]中的方案相同.文献[59]给出了首个对超级攻击者安全的、不使用 Priring 的无证书签名方案.

对上面提到的主要方案,列表比较见表 2,其中:模型栏的 Huang、普通、强、超级分别指在 Huang 的模型下安全、对普通、强或超级攻击者安全;ROM 和 STM 分别指随机预言模型和标准模型.p:双线性对;s:点乘运算;e:指数运算;$|G_1|$:G_1 中元素的长度;$|G_2|$:G_2 中元素的长度;$|q|$:Zq 中元素的长度.

2.3.6 有待深入研究的问题

对于无证书签名,仍有下列几个值得进一步深入研究的问题:

(1) 如何构造高效的在标准模型下可证明安全无证书签名方案?

目前为止,标准模型下可证明安全无证书签名构造方法都基于 Waters 哈希函数,而使用此方法将会导致方案有很长的系统参数并且需要较多的 Pairing 计算.显然,这些方案不适合那些存储能力及计算能力有限的实体(比如无线网路及传感器网络中的节点);

(2) 如何构造高效的,能抵抗超级攻击者的无证书短签名方案?

高效短签名尤其适合存储能力及带宽受限的环境.现有的无证书短签名方案都只在一个较弱的模型下得到了证明(证明不严谨或第 1 类攻击者为普通攻击者),然而在现实世界中,往往会出现用户使用私钥不当的情

况.例如,用户更换了他的秘密值而用原来的签名算法进行签名,那么就容易遭到 Shim 方法[49]的攻击;

(3) 如何构造高效的具有特殊性质的无证书签名方案?

普通的无证书签名在方案设计、安全性分析上已经取得很大的进展,然而对于具有特殊性质的无证书签名(环签名、聚合签名、代理签名、不可否认签名、群签名等)研究还不够深入.例如在环签名方面,一个真正意义上可证明安全的环签名方案由 Zhang 等人[61]给出,该方案在计算上相当高效,然而签名长度较长;Chow 等人[62]的方案由于采用了较弱的安全模型,其安全性还有待探讨.此外,该方案验证算法效率较低.在聚合签名方面,Gong 等人[63]提出了两个无证书的聚合签名方案,其安全性只在一个较弱的模型下得到了证明;随后,文献[64]强化了无证书聚合签名的安全性定义,并提出了更为高效的无证书聚合签名方案;文献[65−69]进一步提高了聚合的效率.无证书代理签名方案最早由 Li 等人[70]提出,但无安全性证明,在文献[71−73]中被攻破.文献[74]给出了无证书代理签名方案的一个强的安全模型和一个可证明安全的方案.文献[75]讨论了不可否认的无证书签名.

Table 2 Comparison of certificateless signature schemes

表 2 无证书签名方案比较

Scheme	Key length		Computational cost		Signature length	Security model	Attack or weakmess
	Secret key	Public key	Signing	Verification			
Ref.[3]	$\|G_1\|$	$2\|G_1\|$	$1p+3s$	$4p+1e$	$1\|G_1\|+1\|q\|$	No proof	Ref.[37]
Ref.[15]	$1\|q\|+2\|G_1\|$	$2\|G_1\|$	$6s$	$6p$	$3\|G_1\|$	Strong-STM	—
Ref.[37]	$\|G_1\|$	$2\|G_1\|$	$1p+3s$	$4p+1e$	$1\|G_1\|+1\|q\|$	Huang-ROM	Ref.[42]
Ref.[38]	$1\|G_1\|$	$1\|G_1\|$	$2s$	$2p+1s$	$2\|G_1\|$	Huang-ROM	Refs.[39−41]
Ref.[42]	$1\|q\|+1\|G_1\|$	$1\|G_1\|$	$3s$	$4p$	$2\|G_1\|$	Strong-ROM	—
Ref.[43]-1	$1\|q\|+1\|G_1\|$	$1\|G_1\|$	$1s$	$3p$	$1\|G_1\|$	Ordinary-ROM	—
Ref.[43]-2	$1\|q\|+1\|G_1\|$	$1\|G_1\|$	$3s+1e$	$2p+2s+1e$	$1\|G_1\|+2\|q\|$	Super-ROM	—
Ref.[44]	$1\|G_1\|$	$1\|G_1\|$	$2s$	$3p+1s$	$2\|G_1\|$	No proof	Ref.[45]
Ref.[46]	$1\|q\|$	$1\|q\|+1\|G_1\|$	$1s$	$5s$	$2\|G_1\|$	No proof	—
Ref.[47]-1	$1\|G_1\|$	$1\|G_1\|$	$2s$	$2p+2s$	$2\|G_1\|$	Huang-ROM	—
Ref.[47]-2	$1\|G_1\|$	$1\|G_1\|$	$1p+1s$	$1p+2s+1e$	$1\|G_2\|+1\|G_1\|$	Huang-ROM	—
Ref.[48]	$1\|q\|+2\|G_1\|$	$1\|G_1\|$	$9s$	$6p$	$4\|G_1\|$	Huang-STM	—
Ref.[50]	$1\|q\|+1\|G_1\|$	$1\|G_1\|$	$1s$	$1p+1s$	$1\|G_1\|$	Huang -ROM	Ref.[51]
Ref.[52]	$1\|q\|+1\|G_1\|$	$2\|G_1\|$	$1s$	$2p+1s$	$1\|G_1\|$	Ordinary -ROM	—
Ref.[53]	$1\|q\|+1\|G_1\|$	$1\|G_2\|$	$1s+2e$	$1p+3e$	$1\|G_1\|+2\|q\|$	Strong-ROM	—
Ref.[54]	—	—	—	—	—	Super	—
Ref.[55]	$1\|q\|+1\|G_1\|$	$1\|G_1\|$	$3s$	$2p+2s$	$2\|G_1\|$	Super-ROM	—
Ref.[56]	$1\|q\|+1\|G_1\|$	$1\|G_1\|$	$1s+1e$	$3p+1e$	$1\|G_1\|+1\|q\|$	Super-ROM	—

3 无证书密钥协商

与无证书加密和签名一样,无证书密钥协商[26,76−98]首先也是由 AL-Riyami 提出[26].为提高文献[26]中协议的计算效率,Mandt[76]提出两个新的协议. Xia[77],Gao[78]指出了 Mandt 方案的安全漏洞,并提出了改进方案.Catalano[79]研究了匿名无证书密钥协商及其在洋葱路由方面的应用.Wang[80]引进签名,提出了一个无证书认证密钥协商协议,签名的使用无疑将增加协议的计算代价,同时在安全性方面也有不足[81].文献[82,85]相继提出了几个无证书双方密钥协商方案,相对于第 1 个方案,这些方案在计算效率上有一定提高.但在安全性方面,所有这些文献都没有给出一个合理的无证书双方密钥协商的安全模型以及严格的形式化证明,其中,文献[83,84]中的方案已被攻击[81].

文献[86]首先对无证书双方密钥协商的安全模型做了研究.随后,Lippold 等人[87]也提出了适用于无证书双方密钥协商的安全模型.其模型描述较为详尽,充分考虑了无证书体制下攻击者的各种能力.在他们的模型里,一个会话密钥的产生需要依赖参与方的 3 类秘密信息:部分私钥、秘密值、临时随机数.称一个双方无证书密钥协商协议是安全的,是指在参与协议的双方各有一个秘密信息没有泄露的情况下,攻击者不能以不可忽略的概率区分一个真实的会话密钥和一个随机值.而且他们的模型是强的——即使攻击者已经替换了用户的公钥,挑战者同样能够正确地回答会话密钥泄露询问(session key reveal query).文献[87]还给出了一个只需要一轮的双方密钥协商协议,但是每一个用户需要计算 5 个模指数运算和 10 个双线性对才能得到协商的密钥.因此计算

代价太大,实用性不强.Swanson[88]基于文献[86]和扩展的 CK 模型(extended Canetti-Krawczyk model,简称 eCK)引入了无证书双方密钥协商的另一安全模型.相比而言,Lippold 等人的模型在理论上更强.两模型的主要区别在于对替换后的公钥的使用.Swanson[88]在其安全模型下对先前提出的无证书双方密钥协商协议进行了分析,指出所有这些协议都存在安全漏洞.近期,Hou 等人[89−92]又提出了几个无证书双方密钥协商协议,但都缺少在合理安全模型下严格的形式化证明.

在合理安全模型下可证明安全、高效、实用的双方无证书密钥协商协议还需深入探讨.

对于无证书三方密钥协商和群体密钥协商也有一些研究成果[93−98].Gao 等人[93]以基于身份的三方密钥协商为基础,利用双线性对设计了一个效率较高的三方无证书密钥协商协议.Heo[95]基于树结构提出了一个无证书群体密钥协商协议,但不能满足完备前向安全等属性.Lee[96]给出的群体密钥协商协议由于使用了 Shi 等人[84]的有安全缺陷的双方协商协议,因而其安全性是不可信赖的.Cao 等人[94]基于门限秘密分享提出了一个无证书群体密钥协商协议,其中采用签名来实现认证功能,但安全性证明不够严格.Geng 等人[97]对文献[94]中的协议重新进行了分析,指出了其中的几个安全缺陷;同时,借助于批验证签名提出了一个改进的群体密钥协商协议.文献[98]给出了另一个无证书群体密钥协商协议,但计算效率不够高.

相对于无证书双方密钥协商而言,对无证书三方及群体密钥协商的研究还远不够深入.主要问题表现在:

1) 公开文献中,还没有比较合理、描述详尽的安全模型.大部分协议的分析都是对照一条条安全属性来设计攻击方式,看能不能达到攻击目的,即使有些论文有模型,描述也是不严谨的;
2) 缺少通信和计算代价小的高效协议.现有的三方和群体无证书密钥协商协议大多借助于双线性对和签名,需要较大的计算和通信代价,这对很多实际应用来说是不够的.

因此,定义无证书三方及群体密钥协商协议的合理的安全模型、给出有形式化安全证明的高效协议,仍然是无证书密码体制研究中值得继续深入探讨的问题.

4 无证书密码体制的其他方面

4.1 无证书签密及多接收者签密

签密把公钥加密和数字签名有机结合在一起,可在一个合理的逻辑步骤内同时完成对消息的加密和签名.在无证书签密[99−111]方面,文献[99−101]给出了几个具体方案.但是,文献[102]指出这几个方案都是不安全的,并且给出了攻击方法.文献[103]提出构造高效无证书签密方案的方法,但未看到对安全性的详细论证.Li 等人[104]讨论了无证书混合签密,文献[105]指出文献[104]中的签密方案是存在可伪造的.Xie 等人[106]提出了一种无证书签密方案.Liu 等人[107]首先研究了在标准模型下安全的无证书签密方案,但其安全性证明不够严格,文献[108]对其方案给出了攻击方法.

无证书多接受签密方案首先由 Selvi 等人在文献[109]中进行了研究,他们提出了一个方案,并对安全性进行了分析.之后又在文献[110]中指出原方案对第 1 类攻击者是脆弱的,并提出了改进方案.该改进方案又被文献[111]攻破.

性能优良、可证明安全的无证书签密以及多接收者签密方案还需进一步研究.

4.2 无证书门限体制

近两年,在无证书门限体制[112−120]方面已有一些工作进展.Long 等人[112]首先研究了无证书门限解密问题,他们提出了在随机预言模型下具有选择密文安全性的一个无证书门限解密方案.Zhang[113],Yang 等人[114]分别提出了在标准模型下安全的无证书解密方案.两方案均未提供解密份额有效性检验方法,这会导致合成算法因使用无效解密份额而输出不正确的明文信息.同时,其安全性证明都不够严谨,其安全性是存在问题的.文献[114]中,方案的系统主密钥和用户公钥很长.文献[115]研究了无证书门限密钥封装机制.

Wang 等人[116]首先探讨了无证书门限签名,其中的安全模型不强,所采用的密钥分享方法不能检测某些欺骗行为,且签名过长.Yuan 等人[117]在一个较强的安全模型下提出了一个可证明安全的无证书门限签名方案.

Xiong 等人[118,119]在标准模型下研究了无证书门限签名,安全模型较弱,其签名预言器在签名人公钥被替换后就无法提供有效的签名.其中的方案是不安全的,攻击者可任意伪造签名.另外,其完整密钥生成与分享算法也存在缺陷,其使用的逆向插值可能导致门限值降低.文献[120]对无证书门限环签名进行了研究.

研究安全高效的无证书门限解密和门限签名方案,在群体保密通信以及防止单点失败等方面有重要意义.合理且强的安全模型、运行高效的门限解密以及签名方案,尤其是标准模型下安全的无证书门限解密及签名方案,仍然是无证书体制下值得深入研究的课题.

5 结束语

新型的无证书公钥密码体制经过几年的研究,已经取得了一些有意义的成果.本文全方位地就其中的主要成果进行了总结整理,从无证书加密、签名、密钥协商、签密与多接受者加密,以及门限体制等几个方面分析了目前的研究现状,对部分成果进行了评述,指出了其中的不足.我们看到,在安全性方面,现有文献中的不少方案或协议由于安全模型不合理,或证明不严谨,而存在安全缺陷.同时,我们也探讨了在每一个方面需要进一步深入研究的问题.需要特别指出的是,鉴于包括侧信道攻击在内的形形色色的密钥泄露攻击对密码系统安全性的威胁,以及新的计算技术如量子计算等对现代密码学的挑战,我们认为,对能抵抗密钥泄露攻击(leakage resilient)以及在量子计算下安全的无证书密码体制的研究,将是非常有意义和富有挑战性的新课题.

致谢 衷心感谢评审专家提供的建议与信息.

References:

[1] Diffie W, Hellman ME. New directions in cryptography. IEEE Trans. on Information Theory, 1976,22(6):644−654.

[2] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakely GR, Chaum D, eds. Advances in Cryptology-Crypto'84. LNCS 196. Heidelberg: Springer-Verlag, 1985. 47−53.

[3] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452−473.

[4] Cheng ZH, Comley R. Efficient certificateless public key encryption. Report, 2005/012, Cryptology ePrint Archive, London: Middlesex University, 2005. http://eprint.iacr.org/2005/012

[5] Dent AW. A survey of certificateless encryption schemes and security models. Int'l Journal of Information Security, 2007,7(5): 349−377. [doi: 10.1007/s10207-008-0055-0]

[6] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing. In: Zhou J, Lopez J, Deng RH, Bao F, eds. Proc. of the ISC 2005. LNCS 3650, Heidelberg: Springer-Verlag, 2005. 134−148.

[7] Rackoff C, Simon DR. Non-Interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum J, ed. Proc. of the Crypto'91. LNCS 576, Heidelberg: Springer-Verlag, 1991. 433−444. [doi: 10.1007/3-540-46766-1_35]

[8] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Ashby V, Denning D, eds. Proc. of the ACM CCS'93. New York: ACM Press, 1993. 62−73. [doi: 1145/168588.168596]

[9] Al-Riyami SS, Paterson KG. CBE from CL-PKE: A generic construciton and efficient schemes. In: Vaudenay S, ed. Proc. of the PKC 2005. LNCS 3386, Berlin: Springer-Verlag, 2005. 398−415. [doi: 10.1007/978-3-540-30580-4_27]

[10] Libert B, Quisquater JJ. On constructing certificateless cryptosystems from identity based encryption. In: Yung M, Dodis Y, Kiayias A, Malkin TG, eds. Proc. of the PKC 2006. LNCS 3958, New York, Berlin: Springer-Verlag, 2006. 474−490.

[11] Zhang ZF, Feng DG. On the security of a certificateless public-key encryption. Report 2005/426, Cryptology ePrint Archive, 2005. http://eprint.iacr.org/2005/426

[12] Shi YJ, Li JH, Shi JJ. Constructing efficient certificateless public key encryption with pairing. Int'l Journal of Network Security, 2008,6(1): 26−32.

[13] Sun YX, Zhang FT, Baek J. Strongly secure certificateless public key encryption without pairing. In: Zhou J, Lopez J, Deng RH, Bao F, eds. Proc. of the CANS 2007. LNCS 4856, Berlin: Springer-Verlag, 2007. 194−208. [doi: 10.1007/978-3-540-76969-9_13]

[14] Lai JZ, Kou WD. Self-Generated-Certificate public key encryption without pairing. In: Okamoto T, Wang X, eds. Proc. of the PKC 2007. LNCS 4450, Berlin: Springer-Verlag, 2007. 476−489. [doi: 10.1007/978-3-540-71677-8_31]

[15] Liu JK, Au MH, Susilo W. Self-Generated-Certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In: Bao F, Miller S, Deng R, Samarati P, eds. Proc. of the 2nd ACM Symp. on Information, Computer and Communications Security. New York: ACM Press, 2007. 273−283. [doi:10.1145/1229285.1266994]

[16] Wang XA, Huang XY, Yang XY. Further observations on certificateless public key encryption. In: Yung M, Liu P, Lin D, eds. Proc. of the Inscrypt 2008. LNCS 5487, Berlin: Springer-Verlag, 2009. 217−239. [doi: 10.1007/978-3-642-01440-6_18]

[17] Sun YX, Zhang FT. Secure certificateless encryption with short ciphertext. Chinese Journal of Electronics, 2010,19(2):313−318.

[18] Lai JZ, Deng RH, Liu SL, Kou WD. RSA-Based certificateless public key encryption. In: Bao F, Li H, Wang G, eds. Proc. of the ISPEC 2009. LNCS 5451, Berlin: Springer-Verlag, 2009. 24−34. [doi: 10.1007/978-3-642-00843-6_3]

[19] Selvi SSD, Vivek SS, Rangan CP.CCA2 secure certificateless encryption schemes based on RSA. Report 2010/459, Cryptology ePrint Archive, 2010. http://eprint.iacr.org/2010/459

[20] Lee YR, Lee HS. An authenticated certificateless public key encryption scheme. Trends in Mathematics Information Center for Mathematical Sciences, 2005,8(1):177−187.

[21] Ju HS, Kim DY, Lee DH, Lim J, Chun K. Efficient revocation of security capability in certificateless public key cryptography. In: Khosla R, Howlett RJ, Jain LC, eds. Proc. of the KES 2005. LNAI 3682, Heidelberg: Springer-Verlag, 2005. 453−459.

[22] Park JH, Choi KY, Hwang JY, Lee DH. Certificateless public key encryption in the selective-ID security model (without random oracles). In: Takagi T, Okamoto T, Okamoto E, Okamoto T, eds. Proc. of the Pairing 2007. LNCS 4575, Heidelberg: Springer-Verlag, 2007. 60−82. [doi: 10.1007/978-3-540-73489-5_5]

[23] Dent AW, Libert B, Paterson KG. Certificateless encryption schemes strongly secure in the standard model. In: Cramer R, eds. Proc. of the PKC 2008. LNCS 4939, Heidelberg: Springer-Verlag, 2008. 344−359. [doi: 10.1007/978-3-540-78440-1_20]

[24] Au MH, Chen J, Liu J K, Mu Y, Wong DS, Yang G. Malicious KGC attack in certificateless cryptography. In: Bao F, Miller S, eds. Proc. of the ACM Symp. on Information, Computer and Communications Security (ASIACCS 2007). New York: ACM Press, 2007. 302−311. [doi: 10.1145/1229285.1266997]

[25] Hwang YH, Liu JK, Chow SSM. Certificateless public key encryption secure against malicious KGC attacks in the standard model. Journal of Universal Computer Science, Special Issue on Cryptography in Computer System Security, 2008,14(3):463−480.

[26] Al-Riyami SS. Cryptographic schemes based on elliptic curve pairings [Ph.D. Thesis]. University of London, 2004.

[27] Yum DH, Lee PJ. Generic construction of certificateless encryption. In: Laganà A, Gavrilova M, Kumar V, Mun Y, Tan CJK, Gervasi O, eds. Proc. of the ICCSA 2004. LNCS 3043, Fukuoka, Heidelberg: Springer-Verlag, 2004. 802−811. [doi: 10.1007/978-3-540-24707-4_93]

[28] Galindo D, Morillo P, Ràfols C. Breaking Yum and Lee generic constructions of certificateless and certificate-based encryption schemes. In: Atzeni AS, Lioy A, eds. Proc. of the EuroPKI 2006. LNCS 4043, Heidelberg: Springer-Verlag, 2006. 81−91. [doi: 10.1007/11774716_7]

[29] Bentahar K, Farshim P, Malone-Lee J, Smart NP. Generic constructions of identity-based and certificateless KEMs. Report 2005/058, Cryptology ePrint Archive, 2005. http://eprint.iacr.org/2005/058

[30] Bentahar K, Farshim P, Malone-Lee J, Smart NP. Generic constructions of identity-based and certificateless KEMs. Journal of Cryptology, 2008,21(2):178−199. [doi: 10.1007/s00145-007-9000-z]

[31] Cheng ZH, Chen LQ, Ling L, Comley RA. General and efficient certificateless public key encryption constructions. In: Takagi T, Okamoto T, Okamoto E, Okamoto T, eds. Proc. of the Pairing 2007. LNCS 4575, Heidelberg: Springer-Verlag, 2007. 83−107. [doi: 10.1007/978-3-540-73489-5_6]

[32] Huang Q, Wong DS. Generic certificateless encryption in the standard model. In: Miyaji A, Rannenberg K, eds. Proc. of the IWSEC 2007. LNCS 4572, Heidelberg: Springer-Verlag, 2007. 278−291. [doi: 10.1007/978-3-540-75651-4_19]

[33] Huang Q, Wong DS. Generic certificateless encryption secure against malicious-but-passive KGC attacks in the standard model. Journal of Computer Science and Technology, 2010,25(4):807−826. [doi: 10.1007/s11390-010-9367-4]

[34] Huang Q, Wong DS. Generic certificateless key encapsulation mechanism. In: Pieprzyk J, Ghodosi H, Dawson E, eds. Proc. of the ACISP 2007. LNCS 4586, Heidelberg: Springer-Verlag, 2007. 215−229. [doi: 10.1007/978-3-540-73458-1_17]

[35] Lippold G, Boyd C, Nieto JMG. Efficient certificateless KEM in the standard model. In: Lee D, Hong S, eds. Proc. of the ICISC 2009. LNCS 5984, Heidelberg: Springer-Verlag, 2010. 34−46. [doi: 10.1007/978-3-642-14423-3_3]

[36] Abe M, Kiltz E, Okamoto T. Compact CCA-secure encryption for messages of arbitrary length. In: Jarecky S, Tsudik G, eds. Proc. of the PKC 2009. LNCS 5443, Heidelberg: Springer-Verlag, 2009. 377−392. [doi: 10.1007/978-3-642-00468-1_21]

[37] Huang XY, Susilo W, Mu Y, Zhang FT. On the security of certificateless signature schemes from asiacrypt 2003. In: Desmedt YG, Wang H, Mu Y, Li Y, eds. Proc. of the CANS 2005. LNCS 3810, Heidelberg: Springer-Verlag, 2005. 13−25. [doi: 10.1007/11599371_2]

[38] Yap W, Heng S, Goi B. An efficient certificateless signature scheme. In: Zhou X, Sokolsky O, Yan L, Jung ES, Shao Z, Mu Y, Lee DC, Kim D, Jeong YS, Xu CZ, eds. Proc. of the EUC Workshops 2006. LNCS 4097, Heidelberg: Springer-Verlag, 2006. 322−331. [doi: 10.1007/11807964_33]

[39] Park JH. An attack on the certificateless signature scheme from EUC Workshops 2006. Report 2006/442, Cryptology ePrint Archive, 2006. http://eprint.iacr.org/2006/442.pdf

[40] Zhang ZF, Feng DG. Key replacement attack on a certificateless signature scheme. Report 2006/453, Cryptology ePrint Archive, 2006. http://eprint.iacr.org/2006/453.pdf

[41] Li JG, Huang XY, Mu Y, Wu W. Cryptanalysis and improvement of an efficient certificateless signature scheme. Journal of Communications and Networks, 2008,10(1):10−17.

[42] Zhang ZF, Wong DS, Xu J, Feng DG. Certificateless public-key signature: Security model and efficient construction. In: Zhou J, Yung M, Bao F, eds. Proc. of the ACNS 2006. LNCS 3989, Heidelberg: Springer-Verlag, 2006. 293−308. [doi: 10.1007/11767480_20]

[43] Huang XY, Mu Y, Susilo W, Wong DS, Wu W. Certificateless signature revisited. In: Pieprzyk J, Ghodosi H, Dawson E, eds. Proc. of the ACISP 2007. LNCS 4586, Heidelberg: Springer-Verlag, 2007. 308−322. [doi: 10.1007/978-3-540-73458-1_23]

[44] Gorantla MC, Saxena A. An efficient certificateless signature scheme. In: Hao Y, Liu J, Wang YP, Cheung YM, Yin H, Jiao L, Ma J, Jiao JC, eds. Proc. of the CIS 2005. LNAI 3802, Heidelberg: Springer-Verlag, 2005. 110−116. [doi: 10.1007/11596981_16]

[45] Cao XF, Paterson KG, Kou WD. An attack on a certificateless signature scheme. Report 2006/367, Cryptology ePrint Archive, 2006. http://eprint.iacr.org/2006/367.pdf

[46] Harn L, Ren J, Lin CL. Design of DL-based certificateless digital signatures. Journal of Systems and Software, 2009,82(5):789−793. [doi: 10.1016/j.jss.2008.11.844]

[47] Choi KY, Park JH, Hwang JY, Lee DH. Efficient certificateless signature schemes. In: Katz J, Yung M, eds. Proc. of the ACNS 2007. LNCS 4521, Heidelberg: Springer-Verlag, 2007. 443−458. [doi: 10.1007/978-3-540-72738-5_29]

[48] Yuan YM, Li D, Tian LW, Zhu HS. Certificateless signature scheme without random oracles. In: Park JH, *et al*., eds. Proc. of the ISA 2009. LNCS 5576, Heidelberg: Springer-Verlag, 2009. 31−40. [doi: 10.1007/978-3-642-02617-1_4]

[49] Shim KA. Breaking the short certificateless signature scheme. Information Sciences, 2009,179(3):303−306. [doi: 10.1016/j.ins.2008.08.024]

[50] Du HZ, Wen QY. Efficient and provably-secure certificateless short signature scheme from bilinear pairings. Computer Standards & Interfaces, 2009,31(2):390−394. [doi: 10.1016/j.csi.2008.05.013]

[51] Fan CT, Hsu RH, Ho PH. Cryptanalysis on Du-Wen certificateless short signature scheme. In: Kim KJ, *et al*., eds. Proc. of the 4th Joint Workshop on Information Security (JWIS 2009). Kaohsiung: Institute of Electrical and Electronics Engineers Inc, 2009. 1−7.

[52] Tso RL, Yi X, Huang XY. Efficient and short certificateless signature. In: Franklin MK, Hui LCK, Wong DS, eds. Proc. of the CANS 2008. LNCS 5339, Heidelberg: Springer-Verlag, 2008. 64−79. [doi: 10.1007/978-3-540-89641-8_5]

[53] Zhang L, Zhang FT, Zhang FG. New efficient certificateless signature scheme. In: Denko M, *et al*., eds. Proc. of the EUC Workshops 2007. LNCS 4809, Heidelberg: Springer-Verlag, 2007. 692−703. [doi: 10.1007/978-3-540-77090-9_64]

[54] Hu BC, Wong DS, Zhang ZF, Deng XT. Key replacement attack against a generic construction of certificateless signature. In: Batten LM, Safavi-Naini R, eds. Proc. of the ACISP 2006. LNCS 4058, Heidelberg: Springer-Verlag, 2006. 235−246.

[55] Zhang L, Zhang FT. A new provably secure certificateless signature scheme. In: Wu J, *et al*., eds. Proc. of the IEEE ICC 2008. Piscataway: Institute of Electrical and Electronics Engineers Inc., 2008. 1685−1689. [doi: 10.1109/ICC.2008.325]

[56] Zhang L, Zhang FT. Certificateless signature and blind signature. Journal of Electronics, 2008,25(5):629−635.

[57] Wan ZM, Lai XJ, Weng J, Liu SL, Long Y, Hong X. Certificateless key-insulated signature without random oracles. Journal of Zhejiang University Science A, 2009,10(12):1790−1800.

[58] Zhang F, Li S, Miao S, Mu Y, Susilo W, Huang X. Cryptanalysis on two certificateless signature schemes, Int'l Journal of Computers, Communications & Control, 2010,5(4):586−591.

[59] Ge AJ, Chen SZ, Huang XY. A concrete certificateless signature scheme without pairings. In: Wang L, *et al*., eds. Proc. of the 2009 Int'l Conf. on Multimedia Information Networking and Security, IEEE Computer Society, 2009. 374−377. [doi: 10.1109/MINES.2009.100]

[60] He DB, Chen JH, Zhang R. Efficient and provably-secure certificateless signature scheme without bilinear pairings. Report 2010/632, Cryptology ePrint Archive, 2010. http://eprint.iacr.org/2010/632.pdf

[61] Zhang L, Zhang FT, Wu W. A provably secure ring signature scheme in certificateless cryptography. In: Susilo W, Liu JK, Mu Y, eds. Proc. of the ProvSec 2007. LNCS 4784, Heidelberg: Springer-Verlag, 2007. 103−121. [doi: 10.1007/978-3-540-75670-5_7]

[62] Chow SS, Yap WS. Certificateless ring signatures. Report 2007/236, Cryptology ePrint Archive, 2007. http://eprint.iacr.org/2007/236.pdf

[63] Gong Z, Long Y, Hong X, Chen KF. Two certificateless aggregate signatures from bilinear maps. In: Feng WY, Gao F, eds. Proc. of the IEEE SNPD 2007, Vol.3. IEEE Computer Society, 2007. 188−193. [doi: 10.1109/SNPD.2007.132]

[64] Zhang L, Zhang FT. Security model for certificateless aggregate signature schemes. In: Wang Y, *et al*., eds. Proc. of the IEEE CIS 2008. Suzhou: IEEE Computer Society, 2008. 364−368. [doi: 10.1109/CIS.2008.9]

[65] Zhang L, Zhang FT. A new certificateless aggregate signature scheme. Computer Communications, 2009,32(6):1079−1085. [doi: 10.1016/j.comcom.2008.12.042]

[66] Zhang L, Qin B, Wu QH, Zhang FT. Novel efficient certificateless aggregate signatures. In: Bras-Amorós M, Høholdt T, eds. Proc. of the 18th Int'l Symp. on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC-18). LNCS 5527, Heidelberg: Springer-Verlag, 2009. 235−238. [doi: 10.1007/978-3-642-02181-7_28]

[67] Chen H, Song WG, Zhao B. Certificateless aggregate signature scheme. In: Xie S, *et al*., eds. Proc. of the 2010 Int'l Conf. on E-Business and E-Government (ICEE). IEEE Computer Society, 2010. 3790−3793. [doi: 10.1109/ICEE.2010.950]

[68] Gong Z, Long Y, Hong X, Chen KF. Practical certificateless aggregate signatures from bilinear maps. Journal of Information Science and Engineering, 2010,26(6):2093−2106.

[69] Zhang L, Qin B, Wu QH, Zhang FT. Efficient many-to-one authentication with certificateless aggregate signatures. Computer Networks, 2010,54(14):2482−2491. [doi: 10.1016/j.comnet.2010.04.008]

[70] Li X, Chen K, Sun L. Certificateless signature and proxy signature schemes from bilinear pairings. Lithuanian Mathematical Journal, 2005,45(1):76−83. [doi: 10.1007/s10986-005-0008-5]

[71] Lu RB, He D, Wang CJ. Cryptanalysis and Improvement of a certificateless proxy signature scheme from bilinear pairings. In: Feng W, Gao F, eds. Proc. of the IEEE SNPD 2007. IEEE Computer Society, 2007. 285−290. [doi: 10.1109/SNPD.2007.166]

[72] Yap WS, Heng SH, Goi BM. Cryptanalysis of some proxy signature schemes without certificates. In: Sauveron D, *et al*., eds. Proc. of the WISTP 2007. LNCS 4462, Heidelberg: Springer-Verlag, 2007. 115−126. [doi: 10.1007/978-3-540-72354-7_10]

[73] Nong Q, Hao YH. Cryptanalysis and improvements of two certificateless signature schemes with additional properties. In: Li Y, ed. Proc. of the 2008 Int'l Symp. on Computer Science and Computational Technology (ISCSCT 2008). Shanghai: IEEE Computer Society, 2008. 54−58. [doi: 10.1109/ISCSCT.2008.46]

[74] Chen H, Zhang FT, Song RS. Certificateless proxy signature scheme with provable security. Journal of Software, 2009,20(3): 692−701 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/20/692.htm [doi: 10.3724/SP.J.1001.2009.00574]

[75] Duan S. Certificateless undeniable signature scheme. Information Sciences, 2008,178(3):742−755. [doi: 10.1016/j.ins.2007.08.009]

[76] Mandt TK, Tan CH. Certificateless authenticated two-party key agreement protocols. In: Okada M, Satoh I, eds. Proc. of the ASIAN 2006. LNCS 4435, Heidelberg: Springer-Verlag, 2008. 37−44. [doi: 10.1007/978-3-540-77505-8_4]

[77] Xia L, Wang SB, Shen JJ, Xu GM. Breaking and repairing the certificateless key agreement protocol from ASIAN 2006. Wuhan University Journal of Natural Sciences, 2008,13(5):562−566.

[78] Gao M, Zhang FT. Key-Compromise impersonation attacks on some certificateless key agreement protocols and two improved protocols. In: Hu Z, ed. Proc. of the 2009 Int'l Workshop on Education Technology and Computer Science (ETCS 2009). Wuhan: IEEE Computer Society, 2009. 62−66. [doi: 10.1109/ETCS.2009.276]

[79] Catalano D, Fiore D, Gennaro R. Certificateless onion routing. In: Gunter C, Ning P, *et al*., eds. Proc. of the CCS 2009. New York: ACM Press, 2009. 1−10. [doi: 10.1145/1653662.1653682]

[80] Wang FJ, Zhang YQ. A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography. Computer Communications, 2008,31(10):2142−2149. [doi: 10.1016/j.comcom.2008.01.054]

[81] Gao M. Research on certificateless two party and tripartite key agreement protocols [MS. Thesis]. Nanjing: Nanjing Normal University, 2009 (in Chinese with English abstract).

[82] Wang SB, Cao ZF, Dong X. Certificateless authenticated key agreement based on the MTI/CO protocol. Journal of Information and Computational Science, 2006,3(3):575−581.

[83] Wang SB, Cao ZF, Wang LC. Efficient certificateless authenticated key agreement protocol from pairings. Wuhan University Journal of Natural Sciences, 2006,11(5):1278−1282. [doi: 10.1007/BF02829251]

[84] Shi YJ, Li JH. Two-Party authenticated key agreement in certificateless public key cryptography. Wuhan University Journal of Natural Sciences, 2007,12(1):71−74. [doi: 10.1007/s11859-006-0194-y]

[85] Wang SB, Cao ZF, Bao HY. Efficient certificateless authentication and key agreement (CL-AK) for grid computing. Int'l Journal of Network Security, 2008,7(3):342−347.

[86] Swanson CM. Security in key agreement: Two-Party certificateless schemes [MS. Thesis]. University of Waterloo, 2008.

[87] Lippold G, Boyd C, Gonzalez NJM. Strongly secure certificateless key agreement. In: Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography—Pairing 2009. LNCS 5671, Heidelberg: Springer-Verlag, 2009. 206−230. [doi: 10.1007/978-3-642-03298-1_14]

[88] Swanson C, Jao D. A study of two-party certificateless authenticated key-agreement protocols. In: Roy B, Sendrier N, eds. Proc. of the INDOCRYPT 2009. LNCS 5922, New Delhi, Heidelberg: Springer-Verlag, 2009. 57−71. [doi: 10.1007/978-3-642-10628-6_4]

[89] Hou M, Xu QL. Constructing secure two-party authenticated key agreement protocol based on certificateless public key encryption scheme. In: Yuan K, *et al*., eds. Proc. of the 4th Int'l Conf. on Computer Science & Education (ICCSE 2009). Nanning: IEEE Computer Society, 2009.1923−1927. [doi: 10.1109/ICCSE.2009.5228215]

[90] Hou MB, Xu QL. On the security of certificateless authenticated key agreement protocol. In: Jin H, *et al*., eds. Proc. of the 4th ChinaGrid Annual Conf. (ChinaGrid 2009). Yantai: IEEE Computer Society, 2009. 974−979.

[91] Hou MB, Xu QL. Key replicating attack on certificateless authenticated key agreement protocol. In: Luo Q, ed. Proc. of the 2009 Asia- Pacific Conf. on Information Processing (APCIP 2009). Shenzhen: IEEE Computer Society, 2009. 574−577. [doi: 10.1109/APCIP. 2009.277]

[92] Hou MB, Xu QL. Two-Party authenticated key agreement protocol from certificateless public key encryption scheme. In: Chung J, *et al*., eds. Proc. of the 2009 Int'l Conf. on Management of e-Commerce and e-Government (ICMeCG). Nanchang: IEEE Computer Society, 2009. 440−444. [doi: 10.1109/ICMeCG.2009.12]

[93] Gao M, Zhang F. An efficient certificateless authenticated tripartite key agreement protocol. In: Wang P, *et al*., eds. Proc. of the Information Systems and Management (ISM 2009). Beijing: IEEE Computer Society, 2009. 1−4.

[94] Cao CJ, Ma JF, Moon S. Provable efficient certificateless group key exchange protocol. Wuhan University Journal of Natural Sciences, 2007,12(1):41−45.

[95] Heo S, Kim Z, Kim K. Certificateless authenticated group key agreement protocol for dynamic groups. In: Shen X, *et al*., eds. Proc. of the Global Telecommunications Conf. (GLOBECOM 2007). Washington: IEEE Computer Society, 2007. 464−468. [doi: 10.1109/GLOCOM.2007.93]

[96] Lee EJ, Lee SE, Yoo K. A certificateless authenticated group key agreement protocol providing forward secrecy. In: Park M, *et al*., eds. Proc. of the IEEE Symp. on Ubiquitous Multimedia Computing (UMC 2008). Hobart: IEEE Computer Society, 2008. 124−129. [doi: 10.1109/UMC.2008.32]

[97] Geng MM, Zhang FT, Gao M. An improved secure certificateless authenticated group key agreement protocol. In: Trajkovic L, Fraser S, eds. Proc. of the 2009 IEEE Int'l Conf. on Intelligent Computing and Intelligent Systems (ICIS 2009), Vol.3. Shanghai: IEEE Computer Society, 2009. 337−341.

[98] Geng M, Zhang F, Gao M. A secure certificateless authenticated group key agreement protocol. In: Wang L, *et al*., eds. Proc. of the 2009 Int'l Conf. on Multimedia Information Networking and Security (MINES 2009), Wuhan: IEEE Computer Society, 2009. 342−346. [doi: 10.1109/MINES.2009.35]

[99] Barbosa M, Farshim P. Certificateless signcryption. In: Abe M, Gligor V, eds. Proc. of the 2008 ACM Symp. on Information, Computer and Communications Security. New York, 2008. 369−372. [doi: 10.1145/1368310.1368364]

[100] Aranha D, Castro R, Lopez J, Dahab R. Efficient certificateless signcryption. 2008. 257−258. http://sbseg2008.inf.Ufrgs.br/proceedings/data/pdf/st03-01-resumo.pdf

[101] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Yu F, Yue G, eds. Proc. of the 2008 Int'l Symp. on Information Science and Engieering (ISISE 2008), Vol.1. Shanghai: IEEE Computer Society, 2008. 661−664. [doi: 10.1109/ISISE. 2008.206]

[102] Selvi SSD, Vivek SS, Rangan CP. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing. In: Bao F, *et al*., eds. Proc. of the Inscrypt 2009. LNCS 6151, 2010. 75−92. [doi: 10.1007/978-3-642-16342-5_6]

[103] Barreto PSLM, Deusajute AM, Cruz ES, Pereira GC, Silva RR. Toward efficient certificateless signcryption from (and without) bilinear pairings. In: Gaspary LP, *et al*., eds. Proc. of the 2008 SBSeg Technical Session 3. Gramado, 2008. 115−125.

[104] Li FG, Shirase M, Takagi T. Certificateless hybrid signcryption. In: Bao F, Li H, Wang G, eds. Proc. of the 2009 Information Security Practice and Experience. LNCS 5451, Heidelberg: Springer-Verlag, 2009. 112−123. [doi: 10.1007/978-3-642-00843-6_11]

[105] Selvi SSD, Vivek SS, Rangan CP. Certificateless KEM and hybrid signcryption schemes revisited. In: Kwak J, *et al*., eds. Proc. of the ISPEC 2010. LNCS 6047, 2010. 294−307. [doi: 10.1007/978-3-642-12827-1_22]

[106] Xie W, Zhang Z. Efficient and provably secure certificateless signcryption from bilinear maps. Report 2010/578, Cryptology ePrint Archive, 2009. http://eprint.iacr.org/2010/578

[107] Liu ZH, Hu YP, Zhang XS, Ma H. Certificateless signcryption scheme in the standard model. Information Sciences, 2010,180(3): 452−464. [doi: 10.1016/j.ins.2009.10.011]

[108] Weng J, Yao GX, Deng RH, Chen MR, Li XX. Cryptanalysis of a certificateless signcryption scheme in the standard model. Information Sciences, 2011,181(3):661−667. [doi: 10.1016/j.ins.2010.09.037]

[109] Selvi SSD, Vivek SS, Shukla D, Chandrasekaran PR. Efficient and provably secure certificateless multi-receiver signcryption. In: Baek J, *et al*., eds. Proc. of the ProvSec 2008. LNCS 5324, Heidelberg: Springer-Verlag, 2008. 52−67. [doi: 10.1007/978-3-540-88733-1_4]

[110] Selvi SSD, Vivek SS, Rangan C. A note on the certificateless multi-receiver signcryption scheme. Report 2009/308, Cryptology ePrint Archive, 2009. http://eprint.iacr.org/2009/308.pdf

[111] Miao SQ, Zhang FT, Zhang L. Cryptanalysis of a certificateless multi-receiver signcryption scheme. In: Furht B, *et al*., eds. Proc. of the 2010 Int'l Conf. on Multimedia Information Networking and Security. 2010. 593−597. [doi: 10.1109/MINES.2010. 130]

[112] Long Y, Chen KF. Certificateless threshold cryptosystem secure against chosen-ciphertext attack. Information Sciences, 2007, 177(24):5620−5637. [doi: 10.1016/j.ins.2007.06.014]

[113] Zhang GY. Certificateless threshold decryption scheme secure in the standard model. In: Zeng L, *et al*., eds. Proc. of the 2nd IEEE Int'l Conf. on Computer Science and Information Technology (ICCSIT 2009). Beijing: IEEE Computer Society, 2009. 414−418. [doi: 10.1109/ICCSIT.2009.5234812]

[114] Yang PY, Cao ZF, Dong XL. Chosen ciphertext secure certificateless threshold encryption in the standard model. In: Yung M, Liu P, Lin D, eds. Proc. of the Inscrypt 2008. LNCS 5487, Beijing, Heidelberg: Springer-Verlag, 2009. 201−216. [doi: 10.1007/978-3-642-01440-6_17]

[115] Long Y, Chen KF. Efficient chosen-ciphertext secure certificateless threshold key encapsulation mechanism. Information Sciences, 2010,180(7):1167−1181. [doi: 10.1016/j.ins.2009.12.008]

[116] Wang LC, Cao ZF, Li XX, Qian HF. Simulatability and security of certificateless threshold signatures. Information Science, 2007,177(6): 1382−1394. [doi: 10.1016/j.ins.2006.08.008]

[117] Yuan H, Zhang FT, Huang XY, Mu Y, Susilo W, Zhang L. Certificateless threshold signature scheme from bilinear maps. Information Sciences, 2010,180(23):4714−4728. [doi: 10.1016/j.ins.2010.07.021]

[118] Xiong H, Qin ZG, Li FG. Simulatability and security of certificateless threshold signatures without random oracles. In: Zhao H, Deb K, Wang Y, eds. Proc. of the 2008 Int'l Conf. on Computational Intelligence and Security (CIS 2008). Suzhou: IEEE Computer Society, 2008. 308−313. [doi: 10.1109/CIS.2008.104]

[119] Xiong H, Li FG, Qin ZG. Certificateless threshold signature secure in thestandard model. Information Sciences, 2010,180(6):1016. [doi: 10.1016/j.ins. 2010.06.010]

[120] Chang S, Wong DS, Mu Y, Zhang ZF. Certificateless threshold ring signature. Information Sciences, 2009,179(20):3685−3696.

附中文参考文献:

[74] 陈虎,张福泰,宋如顺.可证安全的无证书代理签名方案.软件学报,2009,20(3):692−701. http://www.jos.org.cn/1000-9825/20/692.htm [doi: 10.3724/SP.J.1001.2009.00574]

[81] 高猛.无证书双方及三方密钥协商研究[硕士学位论文].南京:南京师范大学,2009.

张福泰(1965－),男,陕西宝鸡人,博士,教授,博士生导师,主要研究领域为密码学,信息安全,网络安全.

耿曼曼(1987－),女,硕士,主要研究领域为密码学,信息安全.

孙银霞(1981－),女,博士生,主要研究领域为密码学,信息安全.

李素娟(1980－),女,博士生,讲师,主要研究领域为密码学,信息安全.

张磊(1982－),男,博士,主要研究领域为密码学,信息安全.