doi:10.11959/j.issn.1000-436x.2016249

WBAN 网络中条件隐私保护的远程用户认证方案

曹进[1]，郑怡清[2]，李晖[1]
（1.西安电子科技大学网络与信息安全学院综合业务网理论与关键技术国家重点实验室，陕西 西安 710126；
2.西安交通大学电子与信息工程学院陕西省计算机网络重点实验室，陕西 西安 710049）

摘 要：提出一种基于无证书群签名的条件隐私保护的远程用户认证方案，实现用户和远程医生间的匿名相互认证；同时当医生发现用户出现紧急情况时，又可以通过群管理员（GM）唯一地来揭露用户的真实身份信息，给予用户及时的救助。提出的认证协议可实现匿名性、可跟踪性、相互认证性、不可否认性和一些其他安全特性。性能分析结果表明该方案更加适合于无线体域网。
关键词：无线体域网；条件隐私保护；远程匿名认证；无证书群签名
中图分类号：TN929 **文献标识码**：A

Conditional privacy-protection remote user authentication mechanism for WBAN

CAO Jin[1], ZHENG Yi-qing[2], LI Hui[1]
(1. State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710126, China;
2. Shaanxi Key Laboratory of Computer Network, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: A conditional privacy-protection remote user authentication scheme based on a certificateless group signature was proposed, which can accomplish the anonymous mutual authentication between the user and the remote doctors. In addition, when the doctors perceived that users were in case of an emergency, the mechanism enabled the only group manager (GM) to expose the real identity information of users and given users timely assistance. The scheme can provide the anonymity, traceability, mutual authentication, non-reputation and some other security features. The performance analysis results show the scheme is more suitable for WBAN.
Key words: wireless body area network, conditional privacy-protection, remote anonymous authentication, certificateless group signature

1 引言

1996 年，Zimmerman 首先提出了无线体域网（WBAN, wireless body area network）的概念，引起了学术界和工业界的广泛关注。2012 年，电气和电子工程师协会（IEEE）为无线体域网通信建立了 IEEE 802.15.6 标准。而近年来，随着无线通信技术和医疗传感器的飞速发展，无线体域网更是蓬勃发展。无线体域网是一种以人体为核心，由植入人体体内或附着于人体表面的传感器组成的无线链路通信网络。无线体域网为人们健康状况的实时监控及远程医疗提供了非常大的便利性，因此，在人口老龄化日益严重的现在有着极大的应用前景和商业价值。越来越多的研究团队加入到探索无线体域网技术在医疗保健领域的优势。例如，哈佛大学研发了用于医疗服务的 CodeBlue 系统[1]，法国 CENS 研究机构开展了 MARSIAN 项目[2]，斯坦福大学和 NASA 阿莫斯实验室联合推出了 LifeGuard 系统[3]。图 1 显示了一个无线体域网的典型医疗应用场景。无线体域网在工作时，通过植入人体体内或附着于人体上的传感器采集人体的生理信息（如血糖、血压、心率等），将其发送给个人的移动设备（如智能手机、

收稿日期：2016-08-31
基金项目：国家自然科学基金资助项目（No.61402354）；111 计划基金资助项目（No.B16037）
Foundation Items: The National Natural Science Foundation of China (No.61402354); China 111 Project (No.B16037)

PDA 等）或者家庭电脑；这些设备将接收到的信息通过基站传输或直接传输到远程医疗应用提供商（AP）；然后医生可以对这些数据进行分析，并对远程的病人进行精确的诊断和治疗。

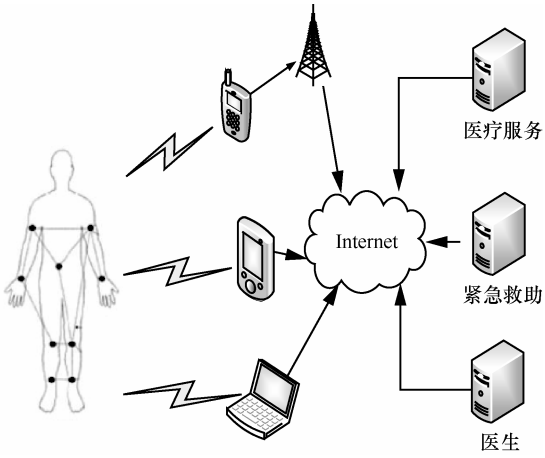


图 1 无线体域网典型医疗应用场景

由于无线体域网被用于临床诊断和测试，实时地监控用户的生理数据，所以，无线体域网中传输的健康数据是十分重要和敏感的。例如，如果无线体域网中传输的数据被篡改，可能会影响医生准确诊断和治疗；或者合法的用户不想让医生知道自己的隐私信息（如姓名和身份证号等），只想匿名地享受无线体域网中的服务。但由于无线体域网独特的性质（如开放的媒体通道、信号噪声、移动终端等），使其在实际应用过程中不可避免地遭受到各类攻击。因此，需要建立一个合适的安全机制来保障用户的隐私信息和实现用户与应用提供商间的相互认证。

近年来，大量针对无线体域网的隐私信息保护方案被提出。目前，关于无线体域网的安全与隐私保护方法主要有 2 类：1) 以生理信息的唯一性为基础；2) 以传统的密码学为基础。

方法 1)是由于人体的生理属性具有差异，因此，可以利用传感器采集到的生理信息来确保数据的安全性和隐私性。Krishna 等[4]提出了一种基于生理信息的密钥协商方案，该方案利用传感器采集到的人体不同部位的生理信息的相似性，通过模糊保险匣方法来实现密钥的协商，因为生理信息具有唯一性，所以在完成密钥协商的同时也就实现了身份认证。Bao 等[5]提出了一种基于心脏搏动间隔的无线体域网轻量级的身份认证方法，该方法详细分析了心脏搏动间隔的随机性、时变性以及同态相似性，设计出了动态个别识别的编码方案。Wang 等[6]提出了一种集成生物特征的安全保护方案，该方案通过小波域隐马尔可夫模型实现身份认证，避免了密钥协商的过程，充分利用生物特征来使该方法具有低功耗和低计算复杂度，很好地实现了信息保护。Zhu 等[7]提出了以心电图为对象的稳定的 R 波峰检测方法，并以 R 波峰检测为基础提出了一种心电信号身份认证方法，提高了身份认证的准确率。虽然这类方法的安全性高，但是生理信息的提取精度不高且过于复杂。该类方法还处于起步阶段。

方法 2)大多数以成熟的密码技术为基础，对现有的技术进行改进，确保 WBAN 中传输和存储数据的安全性和隐私性。Jang 等[8]对无线体域网的安全需求进行了总结并详细地分析了无线体域网所面临的安全威胁，如窃听、中断、数据篡改等，最后以此为依据提出了无线体域网的安全框架。基于对称密码身份认证协议需要在通信实体之间存储预共享密钥。理论上讲，远程用户认证可采用传统公钥密码体制（PKC）实现，但大部分的设计在移动网络中是不可行的，因为公钥密码体制需要进行模幂运算，这可能会消耗比移动设备提供的更多的计算资源。而且传统的公钥密码体制中的证书颁发机构需要存储大量的公钥证书，每次验证之前必须验证证书的有效性，提高了不必要的带宽浪费和时间延迟。考虑到数字证书的创建、颁发、存储、验证和撤销等造成的不利影响，以 Shamir 提出的基于身份的密码系统（IBC）为基础的身份认证协议被提出。Wassim 等[9]提出了一种认证与密钥协商相结合的无线体域网安全方案，以基于身份的密码系统（IBC）方案为基础提出一种身份认证方案，然后使用椭圆曲线上的 DH 密钥交换协议来协商密钥，该方法避免了公钥基础设施和认证中心的使用，具有较低的计算复杂度。Zhao 等[10]提出了一种椭圆曲线密码体制上基于身份的高效匿名认证方案，对比传统的公钥密码体制如 RSA 算法，椭圆曲线有更好的性能，因为它可以用更小的密钥量达到相同的安全性，计算开销小而且基于身份认证不需要证书，非常适合于无线体域网。2003 年，AIRiyami 等[11]提出了无证书的公钥密码系统——CL-PKC，在 CL-PKC 系统中，密钥生成中心（KGC）不再拥有用户的完整私钥，它只是帮助用户产生用户的部分私钥，另一部分私钥是用户自己选取的秘密值，从

而很好地解决了基于身份密码体制的密钥托管问题。随着 CL-PKC 系统的提出，许多基于无证书公钥密码体制的远程认证协议被提出。结合传统的公钥基础设施和基于身份的公钥密码体制中的优点，文献[12]提出了一种无证书远程匿名认证协议，协议使用户和应用提供商能够相互认证对方。而且该方案解决了基于身份的公钥密码体制的密钥分配问题和公钥基础设施的证书管理开销问题。Xiong[13]提出了一种成本有效的可扩展性的无证书远程匿名认证协议，它对文献[12]提出的协议进行了改进，使协议可以抵抗密钥替换问题，而且不需要在客户访问应用提供商之前把客户的账户信息发送到应用提供商，增加了扩展性。Zhang 等[14]为无线体域网提出了一种高效，轻量级的无证书认证协议。这个协议满足匿名、相互认证、无信誉等安全特性。

同时，大量针对无线体域网的无线射频识别系统的匿名认证协议被提出。Bichsel 等[15]提出了基于公钥密码体制的射频识别认证方案，但是存在着高的计算量和管理复杂度。Armknech 等[16]提出了射频识别匿名认证方案，但是它涉及所谓的匿名者的附加设备，它经常与标签进行交互，以确保匿名性和标签的无关联性。Tian 等[17]提出了一种以密文策略为基础的属性加密方案用于无线体域网中，访问结构对数据进行加密，用户属性对数据进行解密。而且不同身份的用户采用不同的访问结构进行加密，实现了医疗数据的细粒度控制访问。Zhang 等[18]提出了一种无线体域网中的多功能加密方案，该方案结合商用的 AES 加密算法与散列算法，同时利用 Shamir 门限方案实现密钥共享，保证了体征参数信息的完整性、机密性与网络的顽健性和容错性。

以上方法能够为 WBAN 中传输和存储数据的安全和隐私性。但是这些方法或多或少都在安全性和性能方面存在着一定的局限性。而且现有的无线体域网安全协议都仅仅停留在如何实现用户与应用提供商之间的远程匿名认证，以保护用户隐私的安全性，却没有考虑到当用户出现紧急情况（如用户的身体突然出现意外状况而用户又是独自一人）时，该如何帮助用户得到及时治疗。

本文为无线体域网提出了一种条件隐私保护的远程用户匿名认证方案。该方案实现合法用户和远程医生之间的相互匿名认证，使合法用户能够最大程度地保护自己的隐私信息。同时，当用户出现紧急情况时，又可以通过群管理员（GM）来唯一地揭露用户的真实身份信息，以及时通知用户的家人或者用户就近的医院，给予用户及时的帮助与治疗。这样能够使无线体域网更好且更安全地提供疾病的预防，检测和对偏远地区患者的监护。

2　预备知识

2.1　无证书签名

文献[11]首次提出了一种新型的密码体制——无证书公钥密码体制。无证书密码体制中有唯一的密钥生成中心（KGC），他持有系统的主密钥，用户的完整私钥是由用户结合 KGC 生成的部分私钥和自己选取的秘密信息生成的，即由于 KGC 无法知道用户的秘密信息，因此 KGC 无法获取得到用户的完整私钥，只有用户自己才知道自己的完整私钥。因此，无证书公钥密码体制很好地解决了基于身份的密码体制的密钥托管问题。同时，用户的公钥是用户结合系统的公开参数和自己选取的秘密信息生成的，因此公钥的认证不再需要证书，有效地克服了传统的公钥基础设施中的证书从产生到撤销的一系列问题和开销。通常，根据文献[11]无证书签名方案一般包含以下几个算法：系统参数产生、部分私钥提取算法、设置秘密值算法、私钥提取算法、设置公钥、签名算法和验证算法。参与算法的主要有 3 个主体：KGC、签名者和验证者。

系统参数产生。由 KGC 完成，是一个概率性多项式时间算法。输入安全参数 k，输出系统参数 *params* 和主密钥 s。KGC 将系统参数 *params* 公开并且将主密钥 s 保密。

部分私钥提取算法。由 KGC 完成的，是一个确定性多项式时间算法。输入系统公开参数 *params*，主密钥 s 和用户的身份 ID，输出一个部分私钥 D，并把 D 通过安全信道传送给用户。

设置秘密值算法。由用户完成的，是一个概率性多项式时间算法。输入系统公开参数 *params* 和用户的身份 ID，输出用户的秘密值 x。

私钥提取算法。由用户完成的，是一个确定性多项式时间算法。输入系统公开参数 *params*，用户的部分私钥 D 和用户的秘密值 x，输出用户的私钥 *SK*。

设置公钥。由用户完成的，是一个确定性多项式时间算法。输入系统公开参数 *params*，用户的部分私钥 D 和用户的秘密值 x，输出用户的公钥 *PK*。

签名算法。由签名者完成的，是一个概率性多项式时间算法。输入系统公开参数 *params*，消息 *m*，用户的身份 ID，用户的私钥 *SK*，输出消息 *m* 的公开可验证的签名。

验证算法。由验证者完成的，是一个确定性多项式时间算法。输入系统公开参数 *params*，消息签名，签名者的公钥 *PK* 和签名者的身份 ID，如果签名验证成功，则输出接受签名，否则输出拒绝签名。

2.2 无证书群签名

群签名是由 Chaum 等[19]在 1991 年提出的。在一个群签名的方案中，一个群体中的任何一个成员都可以以匿名的方式代表整个群体对消息进行签名。群签名和其他数字签名一样，也可以进行公开验证；而且群签名在发生纠纷时，群管理员可以唯一打开群签名来揭露签名者的真实身份。

结合无证书签名和群签名的优点，无证书群签名[20]主要包含以下几个算法。

系统参数的生成。由 KGC 执行，KGC 将生成系统参数和主密钥。

用户公/私钥的生成。用户的完整私钥是由用户结合 KGC 生成的部分私钥和自己选取的秘密信息生成的。同时，由用户自己生成其公钥。

创建群。群管理员产生公钥和私钥，同时设置群公钥。

加入群。想要加入群的用户需要和群管理员执行一系列的协议。认证成功后，群管理员将合法的用户生成其签名所需的用户证书。

群签名。输入用户的消息和私钥，输出消息签名。

验证。验证者验证群签名。

打开。当一个群签名存在争议时，群管理员可以根据存储的信息来确定签名者的真实身份。

成员撤销。群管理员需要去维护成员列表。群成员若想要离开群，需要向群管理员申请，群管理员把相应作废的成员公钥加入到公开的成员撤销列表中。

3 设计的认证协议

本节将详细地介绍无线体域网设计的基于无证书群签名的条件隐私保护的远程用户匿名认证方案。该方案不仅能够保护用户的匿名性，同时又能在用户出现紧急情况时由群管理员来揭露用户的真实身份，给予用户最及时的医疗救助。

3.1 设计目标

本文认为部署在分布式无线体域网应用环境的认证协议应该存在一些权威机构，如密钥生成中心（KGC），可以为网络中不同的主体生成密钥。患者以及医疗服务提供者，为了密钥的分发必须事先和 KGC 联系。因为钥匙是每个人都特定的，它避免了一个身份的认证问题，即确保在无线体域网中身体传感器收集的是一个人的数据而不是多个人的数据。此外，本文假设匿名性是一个基本属性，因为在远程医疗的应用场景中，医生和护士们只需要知道病人的生理信息，而不是其他私人信息（如，姓名和身份证号码等），因此，合法的用户应该被允许能够最大程度地保护他们的敏感信息。但是，本文协议中的匿名性也是在一定条件下的匿名性，因为当出现紧急情况时，用户的真实身份信息唯一能够被管理员安全揭露，以给予用户及时地救助。

在假设的基础上，考虑到无线体域网中的特殊性质，本文设计了这样一个认证方案，它可以达到以下几个目标。

1) 不管是在特定的操作环境还是在无线体域网的网络基础设施中都可以实现匿名。

2) 无线体域网的客户的真实身份在特定条件下可以唯一被管理员揭露。

3) 能够实现无线体域网客户和应用提供商之间的相互认证。

4) 可以为无线体域网的客户提供多于一次的服务。

5) 操作效率高，而产生的计算成本可以忽略不计。

3.2 设计架构

参与认证协议的有 4 种类型的主体：密钥生成中心（KGC）、群管理员（GM）、无线体域网客户端和应用提供商（AP），如图 2 所示。KGC 主要是对系统初始化来生成系统的公开参数和参与用户公私钥的产出。GM 主要是创建群、成员撤销，无线体域网客户端想要加入时也要经过 GM 的认证并为其产生成员证书，而且 GM 是唯一能够有权利打开用户的签名来揭露用户真实身份的主体。在实际运用中，可以把一个范围内的人组成一个群，然后在这个群里选择一个超级管理员来充当 GM。无线体域网客户端一般指那些使用特定的无线体域网终端或应用如 PDA、智能手机、电脑等设备定期地去访问各类由 AP 提供的各种医疗服务，包括病人的监护、医师咨询等服务的主体。而 AP 可以是医院、诊所和医生。

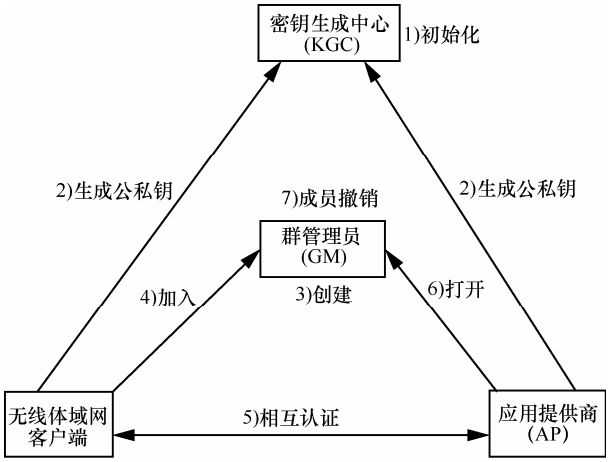


图 2　匿名认证协议中的参与者和工作流程

3.3　认证协议

在本文的协议中，KGC 首先要为无线体域网中每个主体生成公私钥，GM 为每个请求无线体域网的客户端生成签名所需的成员证书。用户为了访问 AP 提供的服务，需要和 AP 之间进行双向的认证，很显然，AP 手中的信息并不允许它恢复用户的真实身份信息，保证了用户的匿名性。同时本文通过 ECDH 来完成用户和 AP 之间的会话密钥的交换。假设被请求的 AP 和请求 G_1 的客户端是同步的。如图 3 所示，本文协议的具体执行可以被正式描述如下。

系统参数的生成。KGC 选择一个安全参数为 l，素数 $q \geqslant 2^l$ 是加法循环群 $(G_1,+)$ 和乘法循环群 $(G_2,\circ)$ 的阶。双线性映射 $e: G_1 \times G_1 \to G_2$。2 个安全的密码散列函数分别为 $H_1:\{0,1\}^* \to G_1^*$，$H_2:\{0,1\}^* \to Z_q^*$。KGC 选择 $s \in {}_R Z_q^*$ 作为系统主密钥，需要保密保管。P 是加法循环群 G_1 的一个生成元，KGC 计算 $P_0 = sP$ 作为系统公钥，并令 $g = e(P,P)$。最后 KGC 将系统的公开参数 $params$= $(G_1, G_2, e, q, P, P_0, g, H_1, H_2)$ 公开。

用户公私钥的生成。用户和 AP 的公私钥的产生都需要 KGC 的参与。按照以下步骤顺序执行。

1) 用户公私钥的生成

① 用户向 KGC 提交自己的身份 $ID_u \in \{0,1\}^*$，KGC 对用户的身份 ID_u 进行认证，认证成功后，KGC 为用户计算其部分私钥 $D_u = sQ_u = sH_1(ID_u)$，然后通过安全信道将 D_u 传送给用户。

② 用户选 $x_u \in Z_q^*$，把 x_u 作为自己的秘密值，即其另一部分的私钥。

③ 用户计算 $P_u = x_u P$，把 P_u 作为自己的公钥。

④ 用户设置自己的完整私钥为（x_u, D_u）。

2) AP 公私钥的生成

① AP 提交身份 $ID_A \in \{0,1\}^*$，KGC 对 AP 的身

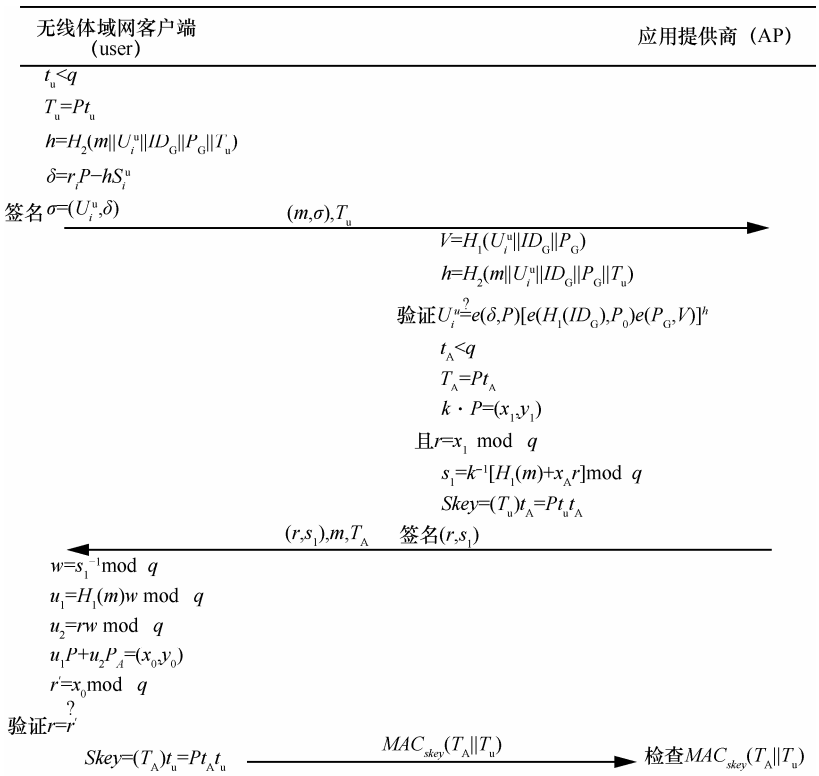


图 3　匿名认证阶段的消息流

份 ID_{A} 进行认证，认证成功后，KGC 为 AP 计算其私钥 $x_{\mathrm{A}}=sQ_{\mathrm{A}}=sH_1(ID_{\mathrm{A}})$，然后通过安全信道将 x_{A} 传送给 AP。

② AP 计算 $P_{\mathrm{A}}=x_{\mathrm{A}}P$，把 P_{A} 作为自己的公钥。

③ AP 设置自己的公私钥对为（$P_{\mathrm{A}},x_{\mathrm{A}}$）。

创建群。GM 身份为 $ID_{\mathrm{G}}\in\{0,1\}^*$，GM 以用户相同的方式去获取自己的公私钥。GM 私钥为（$x_{\mathrm{G}},D_{\mathrm{G}}$），其中，$D_{\mathrm{G}}=sH_1(ID_{\mathrm{G}})$，公钥 $P_{\mathrm{G}}=x_{\mathrm{G}}P$，同时 GM 设置群公钥（$ID_{\mathrm{G}},P_{\mathrm{G}}$）。

加入。用户想加入他所在区域群去访问 AP 的服务，首先他需要与 GM 执行以下协议来加入群，其中，$i=1,2,\cdots,n$。

1) 用户每次随机且独立地选秘密值 $r_i\in{}_RZ_q^*$，秘密值 r_i 将来用作成员签名的私钥，需妥善保存。用户先计算 $U_i^{\mathrm{u}}=g^{r_i}$ 作为成员签名的公钥，然后计算 $h_i'=H_2(U_i^{\mathrm{u}}\|ID_{\mathrm{u}}\|P_{\mathrm{u}})$ 和 $\sigma_i^{\mathrm{u}}=r_iP-h_i'(D_{\mathrm{u}}+x_{\mathrm{u}}H_1(ID_{\mathrm{u}}\|P_{\mathrm{u}}))$，将（$ID_{\mathrm{u}},U_i^{\mathrm{u}},\sigma_i^{\mathrm{u}}$）通过安全信道发送给 GM。

2) GM 收到（$ID_{\mathrm{u}},U_i^{\mathrm{u}},\sigma_i^{\mathrm{u}}$）后，计算 $h_i'=H_2(U_i^{\mathrm{u}}\|ID_{\mathrm{u}}\|P_{\mathrm{u}})$，验证 $U_i^{\mathrm{u}}=e(\sigma_i^{\mathrm{u}},P)\ [e(H_1(ID_{\mathrm{u}}),P_0)e(P_{\mathrm{u}},H_1(ID_{\mathrm{u}}\|P_{\mathrm{u}}))]^{h_i'}$ 是否成立，只有上式成立才给用户颁发成员证书，转向 3)；否则转向 1)，要求重新发送数据，直到上式成立。

3) GM 为用户生成签名所需的成员证书，他对作 U_i^{u} 签名。计算 $S_i^{\mathrm{u}}=D_{\mathrm{G}}+x_{\mathrm{G}}H_1(U_i^{\mathrm{u}}\|ID_{\mathrm{G}}\|P_{\mathrm{G}})$，然后将 S_i^{u} 发送给用户。同时，把 $(ID_{\mathrm{u}},U_i^{\mathrm{u}},\sigma_i^{\mathrm{u}},\ Y_i)$ 加入成员列表，用于保存成员的身份信息和为之后签名的打开和确定签名者真实的身份信息提供依据，其中，$Y_i=e(\sigma_i^{\mathrm{u}},P)$。

4) 用户收到 GM 发给自己的成员证书 S_i^{u} 后，验证 $e(S_i^{\mathrm{u}},P)=e(H_1(ID_{\mathrm{G}}),P_0)\ e(P_{\mathrm{G}},H_1(U_i^{\mathrm{u}}\|ID_{\mathrm{G}}\|P_{\mathrm{G}}))$ 是否成立。只有等式成立才接受成员证书；否则返回 3)，要求 GM 重新发送成员证书，直到上式成立。

当用户与 GM 成功执行完上述步骤，则用户才算正式加入了其所在区域的群，成为群成员，并获得其签名所需的成员证书 S_i^{u}。签名公钥和成员证书的元组 $(U_i^{\mathrm{u}},S_i^{\mathrm{u}})$ 在使用前需妥善保管。

相互认证与密钥协商。

1) 用户→AP

用户要对消息 $m=right$ 签名，$right$ 表示辅助信息，如服务类型和规定时间等，任选他拥有的一个成员证书 S_i^{u} 及对应的签名公/私钥 $\frac{U_i^{\mathrm{u}}}{r_i}$，用户首先选取一个整数 $t_{\mathrm{u}}<q$，然后按照下列步骤生成消息签名。

① 计算 $T_{\mathrm{u}}=Pt_{\mathrm{u}}$

② 计算 $h=H_2\ (m\|U_i^{\mathrm{u}}\|ID_{\mathrm{G}}\|P_{\mathrm{G}}\|T_{\mathrm{u}})$

③ 置 $\delta=r_iP-hS_i^{\mathrm{u}}$

④ 最后输出用户的签名 $\sigma=(U_i^{\mathrm{u}},\delta)$，用户将消息 m，签名 σ 和 T_{u} 一起发送给 AP。当 AP 收到消息 m,签名 σ 和 T_{u} 之后，AP 执行。

⑤ 计算 $V=H_1(U_i^{\mathrm{u}}\|ID_{\mathrm{G}}\|P_{\mathrm{G}})$

⑥ 计算 $h=H_2\ (m\|U_i^{\mathrm{u}}\|ID_{\mathrm{G}}\|P_{\mathrm{G}}\|T_{\mathrm{u}})$，验证 $U_i^{\mathrm{u}}\overset{?}{=}e(\delta,P)\ [e(H_1(ID_{\mathrm{G}}),P_0)e(P_{\mathrm{G}},V)]^h$ 如果验证失败，则 AP 拒绝该签名。否则 AP 接受该签名，然后转向 2)。

2) AP→用户

AP 按以下步骤执行。

① AP 选取一个整数 k，计算 $1\leqslant k\leqslant q-1$；

② AP 选取一个整数 $t_{\mathrm{A}}<q$，计算 $T_{\mathrm{A}}=Pt_{\mathrm{A}}$；

③ 计算 $kP=(x_1,y_1)$ 且 $r=x_1 \bmod q$，如果 $r=0$，则返回①；

④ 计算 $s_1=k^{-1}[H_1(m)+x_{\mathrm{A}}r]\bmod q$，如果 $s_1=0$，则返回①；

⑤ 计算会话密钥 $Skey=(T_{\mathrm{u}})t_{\mathrm{A}}=Pt_{\mathrm{u}}t_{\mathrm{A}}$，AP 将签名（$r,s_1$），$T_{\mathrm{A}}$ 和消息 m 发给用户。

3) 用户→AP

在用户收到 AP 的签名（r,s_1），T_A 和消息 m 之后，用户执行如下步骤。

① 计算 $w=s_1^{-1} \bmod q$；

② 计算 $u_1=H_1(m)w\bmod q$ 和 $u_2=rw\bmod q$；

③ 计算 $u_1P+u_2P_A=(x_0,y_0)$ 和 $r'=x_0 \bmod q$；

④ 验证 $r\overset{?}{=}r'$。

如果验证成功，用户计算会话密钥 $Skey=(T_{\mathrm{A}})t_{\mathrm{u}}=Pt_{\mathrm{A}}t_{\mathrm{u}}$。然后用户给 AP 发送 $MAC_{Skey}[T_{\mathrm{A}}\|T_{\mathrm{u}}]$，当 AP 收到后，用会话密钥 $Skey$ 检查 $MAC_{Skey}[T_{\mathrm{A}}\|T_{\mathrm{u}}]$。如果得到的结果是个负值，AP 将拒绝当前会话。否则用户和 AP 把 $Skey$ 作为以后通信的会话密钥。

打开签名。对于用户的签名 $\sigma=(U_i^u,\delta)$，当 AP 在发现用户身体状况出现危险时，GM 根据之前在成员列表中保存的成员信息 $(ID_{\mathrm{u}},U_i^{\mathrm{u}},\sigma_i^{\mathrm{u}},\ Y_i)$，计算

$h' = H_2(U_i^{\mathrm{u}} \| ID_{\mathrm{u}} \| P_{\mathrm{u}})$，然后验证 $U_i^{\mathrm{u}} = Y_i\,[e(H_1(ID_{\mathrm{u}}), P_0)e(P_{\mathrm{u}}, H_1(ID_{\mathrm{u}} \| P_{\mathrm{u}}))]^{h'}$ 是否成立来确定该签名的真正的签名者。

成员撤销。GM 需要维护成员列表来保存用户的身份信息为打开签名提供依据，对于已经使用过的成员公钥，GM 在相应的成员列表中加上“已使用”的标记。当成员要离开其所在的群，他需要向 GM 提出申请，对成员列表中成员还没有使用的成员公钥 ，GM 为其加上“已作废”的标记，并且只把相应已作废的成员公钥加入到该群的公开的撤销成员列表中。

4　安全性和性能分析

本节通过和现有的协议对比来分析本文协议的安全性和性能。本文的协议确保 KGC 只能生成部分的私钥，避免其假冒合法的用户。本文的协议中只有一个 GM，是唯一能够打开用户的签名去揭露用户真实身份信息的主体，同时本文的协议也可以保证包括 GM 在内的任何人都不能够冒充其他的群成员做出合法的签名。所以这种特性使本文的协议非常适合于实际的无线体域网的应用场景。下面详细地分析本文协议的安全性和性能。

4.1　安全性分析

不可伪造性。假设 CDH 问题是困难的，则本文提出的认证协议满足不可伪造性。

证明　由于本文的认证协议是基于文献[20]中的无证书群签名来设计的，在文献[20]中已经证明若 CDH 问题是困难的，则成员证书和群签名都是不可伪造的。因此在本文的协议中包括 GM 在内的任何人都不能够冒充其他的群成员做出合法的签名，所以本文设计的认证协议同样具有不可伪造性。

匿名性。本文提出的认证协议满足匿名性。它能确保用户在任何操作环境或无线体域网的网络基础设施都可以匿名地访问 AP。

证明　在协议中对于每一个给定的合法用户的签名 $\sigma = (U_i^{\mathrm{u}}, \delta)$，由于 U_i^{u}、δ 都不含有可确定签名者真实身份的信息，而 GM 可以通过其维护的成员列表中保存的成员身份信息来确定签名者的真实身份，所以对除了 GM 外的其他任何人（包括 KGC 在内）来说，要确定真正的签名者的身份信息在计算上是不可行的。因此，本文提出的协议满足匿名性。

不关联性。本文提出的协议满足不关联性。可以确保在不打开用户签名的情况下，无法去确定 2 个不同的签名是否由同一个用户所签。

证明　在本文的协议中，即使是 2 个签名 $\sigma = (U_i^{\mathrm{u}}, \delta)$ 和 $\sigma = (U_j^{\mathrm{u}}, \delta')$，实际上是同一个用户所签，但仍然无法通过计算来确定是同一个用户所签。因为用户每次选择秘密值都是随机的，而且在每次产生签名的时候都使用不同的成员证书，所以 2 次的签名公钥 $U_i^{\mathrm{u}} = g^{r_i}$ 和 $U_j^{\mathrm{u}} = g^{r_j}$ 之间根本没有确定的关系。因此，本文的协议具有不关联性。

可跟踪性。本文提出的协议具有可跟踪性，在紧急情况下本文协议允许 GM 打开用户的签名来揭露用户的真实身份信息。

证明　由不可伪造性可知，只有群成员才能够产生签名。而每一个用户产生的对 AP 的签名都对应该用户唯一的成员证书，每一个成员证书又对应唯一的用户对 GM 的签名。即每个用户对 AP 的签名都对应唯一的用户对 GM 的签名。因此，每个签名都对应唯一的一个签名者。又因为每个签名所对应的签名者给 GM 的签名早在用户对 AP 的签名生成之前已经存在并且被 GM 保存着。因此，签名者不能够阻止一个合法的签名被打开。所以本文的协议具有可跟踪性。当 AP 发现用户身体状况处于紧急情况时，可以告诉 GM，由 GM 来打开用户的签名揭露用户的真实身份信息。

相互认证。无证书群签名和椭圆曲线上的 DSA（ECDSA）确保了在本文的协议中，用户和 AP 之间可以完成相互认证。

证明　只有被请求的 AP 才能够利用从用户那里接收到的 T_{u} 恢复 $h = H_2(m \| U_i^{\mathrm{u}} \| ID_{\mathrm{G}} \| P_{\mathrm{G}} \| T_{\mathrm{u}})$，从而来验证用户发给自己的签名。在 AP 验证了用户是合法的之后，用户也会从 AP 处接收到的 ECDSA 签名 (r, s_1) 进行验证，如果验证成功，则 AP 是用户希望访问请求的那个。任何人如果没有相应的密钥就不可能去产生合法的群签名或者 ECDSA 签名，因此无法去伪装成 AP 或者用户进行欺骗。所以本文的协议满足相互认证性。

不可否认性。在成功的访问之后，因为无证书群签名方案的签名 $\sigma = (U_i^{\mathrm{u}}, \delta)$，所以用户不能否认他/她已经访问过由 AP 提供的服务。

证明　因为群用户是唯一能够产生一个合法的签名 $\sigma = (U_i^{\mathrm{u}}, \delta)$ 的签名者，任何人包括 GM 在内都不能够冒充其他的群成员做出合法的签名，而且

由可跟踪性可知，每一个合法的签名 $\sigma=(U_i^{\mathrm{u}},\delta)$ 都能够被跟踪。所以，用户无法否认他自己产生过的签名。因此本文的协议具有不可否认性。

会话密钥的建立。在相互认证成功之后，AP 和用户需要商议会话密钥来确保接下来数据传输的安全性。

证明 在两者相互验证签名成功后，用户和 AP 通过椭圆曲线上的 DH 密钥交换来生成会话密钥 *Skey* 。即使敌手偷听到所有的会话信息他也无法推断出。而且用户通过发送 $MAC_{Skey}[T_{\mathrm{A}}\|T_{\mathrm{u}}]$ 给 AP 来确定密钥协商的结果，可以抵抗 DoS 攻击。

表 1 显示了不同方案的安全性对比，其中，×表示协议不具有该性质，√表示协议具有该性质。结果表明本文提出的协议安全性更高，比之前所有的协议多了可跟踪性。

表 1 不同协议的安全属性对比

方法	匿名性	可跟踪性	相互认证性	不可否认性	会话密钥的建立
文献[12]方案 1	√	×	√	√	√
文献[12]方案 2	√	×	√	√	√
文献[13]方案	√	×	√	√	√
文献[14]方案	√	×	√	√	√
本文方案	√	√	√	√	√

4.2 性能分析

本节通过和其他的方案进行对比，对本文协议进行了以下 3 个方面的性能分析：计算开销、存储开销和通信开销。

为了达到 1 024 bit RSA 的相同的安全等级，对于基于双线性映射的本文协议，文献[12]和文献[14]的协议，本文采用椭圆曲线 $\frac{E}{F_p}:y^2=x^3+x$，在其之上定义一个 Tate 双线性映射 $e:G_1\times G_1\to G_2$，q 是 160 bit 的素数，p 是一个 512 bit 的素数。基于椭圆曲线密码体制的文献[13]中的协议，为了提供相同的安全等级，本文使用定义在有限域 $F_{2^{163}}$ 上的 Koblitz 椭圆曲线 $y^2=x^3+ax^2+b$，在它上面定义一个椭圆曲线群。其中，a=1，b 是一个 163 bit 的随机素数。并且本文假设用户的身份信息是 2 byte，时间戳是 1 byte，随机数是 4 byte，散列函数是 16 byte。

计算开销。本文只考虑表 2 所列举的计算开销，忽略协议中的模乘和散列函数。其中，BP、E 和 PM 分别表示双线性映射运算、指数运算和椭圆曲线上的点乘。表 2 显示了不同协议的计算开销对比。

表 2 不同协议的计算开销对比

方法	用户	应用提供商
文献[12]方案 1	1E+4PM	1BP+1E+1PM
文献[12]方案 2	1E+4PM	1BP+1E+1PM
文献[13]方案	6PM	5PM
文献[14]方案	2BP+1PM	3PM
本文方案	5PM	2BP+1E+3PM

存储开销。本文只考虑用户的存储需求。文献[13,14]的协议用户需要存储身份信息，公钥和私钥。本文协议中的用户需要存储身份信息、私钥、公钥和签名证书。文献[12]的协议用户需要存储身份信息、私钥、公钥和账户信息。不同协议的存储开销对比如表 3 所示。

通信开销。本文的协议和文献[12~14]的协议一样，都需要 3 次消息交换来完成相互认证和会话密钥的协商。不同协议的通信开销对比如表 3 所示。

表 3 不同协议的存储和通信开销

方法	存储开销/byte	通信开销/byte
文献[12]方案 1	260	341
文献[12]方案 2	284	229
文献[13]方案	84	185
文献[14]方案	86	78
本文方案	214	320

根据不同方案的性能对比，本文协议中用户的计算开销和文献[12]的方案相近，比文献[13, 14]的方案计算开销小。本文协议中用户端的存储开销比文献[13, 14]的方案存储开销大，但是比文献[12]的方案存储开销小。但是本文的协议增加了一个新的可跟踪性，这个是其他所有协议无法提供的。因此，本文提出的协议在安全性和性能上都更适合无线体域网的应用场景。

5 结束语

本文提出了一个基于无证书群签名方案的条件隐私保护的远程用户认证方案。通过和现有其他方案进行对比，本文的协议在保证不过多地降低性能的条件下，可以提供比其他协议更多的一个安全性——可跟踪性。本文的协议不仅能够保证用户的匿名性，而且当用户处于紧急条件下时可以揭露用户的真实身份。安全性分析和性能分析的结果表明本文提出的协议可以提供包括可跟踪性在内的其

他安全性而且达到一个可观的性能。

参考文献：

[1] LORINCZ K, MALAN D J, FULFORD-JONES T R F, et al. Sensor networks for emergency response: challenges and opportunities[J]. Pervasive Computing, IEEE, 2004, 3(4): 16-23.

[2] AXISA F, GEHIN C, DELHOMME G, et al. Wrist ambulatory monitoring system and smart glove for real time emotional, sensorial and physiological analysis[C]//Proceedings of Engineering in Medicine and Biology Society, 26th Annual International Conference of the IEEE. 2004, 1: 2161-2164.

[3] MUNDT C W, MONTGOMERY K N, UDOH U E, et al. A multiparameter wearable physiologic monitoring system for space and terrestrial applications[J]. IEEE Transactions on Information Technology in Biomedicine, 2005, 9(3): 382-391.

[4] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. PSKA: usable and secure key agreement scheme for body area networks[J]. IEEE Transactions on Information Technology in Biomedicine, 2010, 14(1): 60-68.

[5] BAO S D, POON C C Y, ZHANG Y T, et al. Using the timing information of heartbeats as an entity identifier to secure body sensor network[J]. IEEE Transactions on Information Technology in Biomedicine, 2008, 12(6): 772-779.

[6] WANG H, FANG H, XING L, et al. An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks(WBAN)[C]//2011 IEEE International Conference on Proceedings of Communications. 2011: 1-5.

[7] 朱凯. 无线体域网身份认证方法研究[D]. 西安: 西安电子科技大学, 2013.
ZHU K. Research on methods of identity authentication for wireless body area network[D]. Xi'an: Xidian University, 2013.

[8] JANG C, LEE D G, HAN J. A proposal of security framework for wireless body area network[C]//SECTECH'08 International Conference on Security Technology. 2008: 202-205.

[9] DRIRA W, RENAULT E, ZEGHLACHE D. A hybrid authentication and key establishment scheme for wban[C]// 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2012: 78-83.

[10] ZHAO Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem[J]. Journal of Medical Systems, 2014, 38(2): 1-7.

[11] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[M], Advances in Cryptology-Asiacrypt 2003. Springer Berlin Heidelberg, 2003: 452-473.

[12] LIU J, ZHANG Z, CHEN X, et al. Certificateless remote anonymous authentication schemes for wireless body area networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 332-342.

[13] XIONG H. Cost-effective scalable and anonymous certificateless remote authentication protocol[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(12): 2327-2339.

[14] ZHANG L, LIU J, SUN R. An efficient and lightweight certificateless authentication protocol for wireless body area networks[C]//2013 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS). 2013: 637-639.

[15] BICHSEL P, CAMENISCH J, GROß T, et al. Anonymous credentials on a standard java card[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. 2009: 600-610.

[16] ARMKNECHT F, CHEN L, SADEGHI A R, et al. Anonymous authentication for RFID systems[C]//Radio Frequency Identification: Security and Privacy Issues. 2010: 158-175.

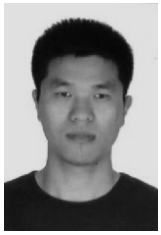
[17] TIAN Y, PENG Y B, YANG Y L, et al. Attribute-based encryption access control scheme in wireless body area networks[J]. Application Research of Computers, 2015, 32(7): 2163-2167.

[18] ZHANG X B, YUAN K G, WU C H, et al. Research of wireless body area network(WBAN) security[C]//The Ninth Academic Annual Conference of China Communication Association. 2012.

[19] CHAUM D, VAN H E. Group signatures[C]//Advances in Cryptology—EUROCRYPT'91. 1991: 257-265.

[20] CHEN H, ZHU C J, SONG R S. Efficient certificateless signature and group signature schemes[J]. Journal of Computer Research and Develpoment, 2010, 47(2): 231-237.

作者简介：



曹进（1985-），男，陕西西安人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为应用密码学，安全协议分析，无线网络安全。

郑怡清（1993-），女，江西上高人，西安交通大学硕士生，主要研究方向为隐私保护。

李晖（1968-）,男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。