无线体域网中高效可撤销的无证书远程匿名认证协议

张顺，范鸿丽，仲红，田苗苗
（安徽大学计算机科学与技术学院，安徽 合肥 230601）

摘 要：为了保证无线体域网（WBAN, wireless body area network）中病人生理数据的安全和隐私，通信双方必须进行相互认证。现有的一些方案使用双线性对导致用户计算代价较大，其采用树形结构进行撤销会导致用户的存储代价较大。为了实现撤销同时降低用户端的代价，构造了基于椭圆曲线的可撤销无证书远程匿名认证协议，基于即时更新时间密钥技术进行撤销。协议满足匿名性，相互认证和会话密钥建立等安全需求。与现有方案相比，实验分析表明认证协议用户端的计算代价和存储代价大幅降低，更适用于资源受限的无线体域网。安全性分析证实了协议在随机预言模型下是安全的。

关键词：无线体域网；匿名认证；可撤销；无证书
中图分类号：TP309，TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018064

Efficient revocable certificateless remote anonymous authentication protocol for wireless body area network

ZHANG Shun, FAN Hongli, ZHONG Hong, TIAN Miaomiao
School of Computer Science and Technology, Anhui University, Hefei 230601, China

Abstract: To ensure the security and privacy of patients' health data in wireless body area network (WBAN), communication parties must be mutual authenticated. Now some bilinear pairings led to a larger computation cost for users and tree structure revocation would lead to larger user storage cost. In order to achieve revocation and reduce the cost of the user side, a novel revocable certificate less remote anonymous authentication protocol for WBAN was proposed by using elliptic curve cryptography and revoke algorithm that could revoke users by updating their time-private-keys. Security requirements including anonymity, mutual authentication and session key establishment were satisfied in proposed scheme. Compared with the existing schemes, the experimental analysis shows that the computation cost and storage cost of the authentication protocol are greatly reduced, which is more suitable for resource-constrained WBAN. Security analysis also shows that the protocol is secure in the random oracle model.

Key words: wireless body area network, anonymous authentication, revocation, certificateless

1 引言

随着传感器技术和无线通信技术的不断发展，无线体域网[1]应运而生，满足了人们对高质量医疗服务的需求。WBAN 由一系列资源受限的穿戴式或嵌入式的传感器节点组成，这些节点能够实时收集病人的生理信息，然后通过智能设备将数据发送到远程应用端进行诊断。图 1 是典型的 WBAN 应用场景，其中 WBAN 中节点收集实时生理数据（心跳、血压等），通过智能设备（个人数字管家、智

收稿日期：2017-05-23；**修回日期**：2018-02-28
通信作者：仲红，zhongh@ahu.edu.cn
基金项目：国家自然科学基金资助项目（No.11301002, No.61572001, No.61502443）；安徽省高校省级优秀青年人才重点基金资助项目（No.2013SQRL006ZD）
Foundation Items: The National Natural Science Foundation of China (No.11301002, No.61572001, No.61502443), Talents Youth Fund of Anhui Province Universities (No.2013SQRL006ZD)

能手机等）将数据发送到远程应用端进行分析诊断。由于收集的敏感生理数据在公共信道上传输，为了保护生理数据的隐私性以及确保用户可以得到及时治疗，在无线体域网认证协议需要满足用户匿名相互认证、不可链接性、不可否认性以及会话密钥建立等安全需求。

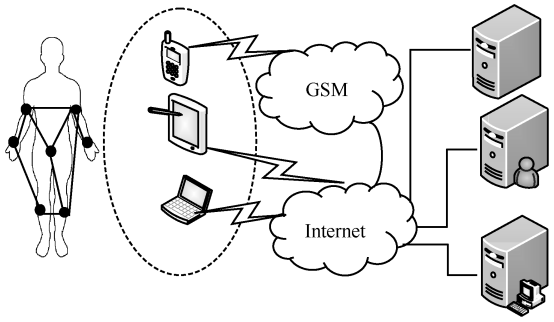


图 1　无线体域网应用场景

首个远程认证协议是由 Lamport[2]提出的，该协议允许移动客户通过公共信道向远程服务器进行身份认证，并且双方可以生成共享会话密钥以保证后期通信的安全。此后，许多远程认证协议被相继提出（如文献[3~7]）。这些协议属于传统公钥密码协和基于身份的密码协议。在传统的公钥密码体制中，客户的公私钥对都是由它自己随机生成，为了确保客户身份和公钥对应关系的真实性，需要证书授权中心（CA, certificate authority）给客户颁发相应的公钥证书。由于证书分发和管理代价较大，因此，这种密码体制不适用于资源受限的 WBAN。基于身份公钥密码体制的思想是由 Shamir[8]提出的，其中，客户的公钥是身份信息，因此，该体制消除了公钥证书。但是在基于身份的密码体制中客户的私钥都是由私钥生成中心（PKG, private key generator）生成的，因此，密钥托管存在问题。为了解决该问题，Al-Riyami 等[9]提出了无证书公钥密码体制。在这种密码体制中客户的私钥由它选择的秘密值和 PKG 生成的部分私钥组成。因此，无证书公钥密码体制不仅消除了公钥证书，还解决了密钥托管问题。

Liu 等[10,11]在 2014 年首次提出了 2 个保护隐私的无证书远程匿名认证协议，由于在协议中服务器需要存储验证表，存在伪造客户的可能性，并且协议不满足前向安全性等安全需求同时也使用了双线性对等操作，客户的计算代价较大。Xiong[12]给出了一种基于无证书加密的远程匿名认证协议，但该协议在客户端使用了较多的点乘操作并且没有考虑到客户和远程应用端的撤销问题，即当客户或远程应用端的密钥泄露或服务到期时，PKG 需要将该客户或远程应用端撤销。否则，服务到期的客户可以继续享受医疗服务，恶意的远程应用端也可以非法收集客户的隐私生理信息。

在无证书公钥系统中，Xiong 等[13]首次提出了在 WBAN 中可撤销的远程匿名认证协议，但该协议使用了大量双线性对以及 map-to-point 散列操作，客户的计算代价太大。此外，协议使用 KUNode 算法[14]进行客户和远程应用端的撤销，树形结构的撤销导致客户的存储开销较大。为了降低客户的开销，Tseng 等[15]提出了一种有效的撤销算法，在该算法中客户的私钥分成 3 个部分：客户选取的秘密值、PKG 生成的部分私钥和 PKG 生成的时间密钥，其中，时间密钥是周期性更新的，因此，可能会出现客户密钥泄露或服务到期发生在更新周期内的情况，而 PKG 无法立即将客户撤销。

基于以上问题，本文基于无证书签名思想，采用椭圆曲线和实时更新时间密钥技术提出了一种高效的可撤销无证书远程匿名认证协议。该协议没有使用双线性对以及 map-to-point 散列操作，客户的计算代价较小。此外，与文献[13]中的协议相比，本文所提协议实现撤销的同时大大降低了客户的存储代价。最后，安全性分析证明该协议在随机预言模型下是安全的。

2　预备知识

本节给出椭圆曲线密码的基本概念和相关困难假设。

2.1　椭圆曲线

素数域 F_p 上的椭圆曲线 E 是由 $y^2 = x^3 + ax + b \mod p$ 上的点集 (x, y) 和一个称为无穷远点 O 组成的，其中，$a, b \in_R F_p$ 并且 $4a^3 + 27b^2 \neq 0 \mod p$。曲线 E 与点加定律“+”形成一个循环加法群 G，无穷远点 O 是单位元。具体定义如下。给定 $P, Q \in G$，则 $P+Q$ 被视为关于 x 轴的反射点 R，其中，R 是曲线 E 和线 l 之间的交叉点。如果 $P \neq Q$，l 由 P 和 Q 决定；如果 $P = Q$，l 表示 $\frac{E}{F_p}$ 的切线。一个点 P 的倍数可以实现为重复的加法，即 $mP = P + P + \cdots + P$。

椭圆曲线的更多信息参考文献[16]。

2.2 困难假设

本文协议的安全性依赖于以下 2 个经典的困难假设。

1) 离散对数问题（DL, discrete logarithm problem）。给定元组 $\{P,xP\}\in G$，在概率多项式时间内找到整数 x 是困难的。

2) 计算 Diffie-Hellman 问题（CDH, computational Diffie-Hellman problem）。给定元组 $\{P,xP,yP\}\in G$，其中，x,y 是 Z_q^* 中未知的整数，在概率多项式时间内计算 xyP 是困难的。

3 系统和安全模型

本节介绍系统模型、安全性需求、可撤销的无证书认证协议以及安全模型。

3.1 系统模型

系统模型如图 2 所示，协议共有 3 个参与方：客户（C）、私钥生成中心（PKG）和远程应用端（AP），其中，C 和 AP 都可能有多个而 PKG 一般只有一个。

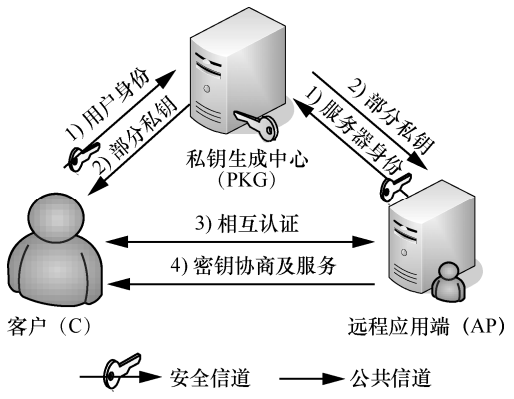


图 2 系统模型

私钥生成中心（PKG）。PKG 被视为 C 和 AP 的注册中心，一般是由半可信的盈利组织担任。为了商业盈利的目的，PKG 可能通过伪装成合法的 AP 来收集病人隐私数据或通过伪装成合法的 C 来获得医疗服务。

客户（C）。客户代表病患。C 配备了一系列传感器节点和智能设备。C 在请求 AP 服务之前需要向 PKG 注册，由 PKG 预设公共参数，部分私钥和时间密钥，其中，部分私钥通过安全信道发送，时间密钥通过公共信道发送。当 PKG 检测到 C 的服务到期或密钥泄露时，需将 C 撤销。

远程应用端（AP）。远程应用端是医疗服务中心，如医院、诊所等。在 AP 给 C 提供远程服务之前同样需要向 PKG 注册并由 PKG 预设公共参数、部分私钥和时间密钥，其中，部分私钥通过安全信道发送，时间密钥通过公共信道发送。当 PKG 检测到 AP 的服务到期或密钥泄露时，需要撤销该 AP。

3.2 安全需求

为了确保 WBAN 环境下的通信安全，认证协议通常需要满足以下安全性需求[11~13]。

1) 客户匿名。为了保护 C 的隐私，包括 PKG 在内的任何第三方都不能通过截获请求消息获得 C 的身份信息。

2) 相互认证。为了确保只有合法的 C 可以获取医疗服务并且只有合法的 AP 可以提供医疗服务，协议需要在 C 和 AP 之间提供相互认证。

3) 不可链接。一个合法的 C 可以向 AP 发出多次服务请求消息，但网络攻击者不能分辨哪些消息来自同一个 C。

4) 会话密钥安全。在完成相互认证之后，C 和 AP 可以建立会话密钥。会话密钥用来保护双方后续的通信安全，所以协议需要保证会话密钥的安全。

5) 前向安全。即使参与方的长期密钥泄露，之前会话中传输的数据依然是安全的，即这些数据不会被泄露。

6) 可撤销。当 C/AP 的私钥泄露或服务到期时，PKG 应能撤销该 C/AP。

3.3 可撤销的无证书远程认证协议

可撤销的无证书远程认证协议主要包括以下几部分，其中，为了叙述方便，将 C 和 AP 统称为用户。

1) 初始化(1^λ)。由 PKG 运行，输入安全参数 1^λ，输出公共参数 $params$、系统主密钥 s 以及系统公钥 P_{pub}。

2)秘密值提取算法(ID)。由用户运行，输入用户身份 ID，输出用户的秘密值 x_{ID}。

3) 公钥提取算法(ID,x_{ID})。由用户运行，输入用户的身份 ID 和秘密值 x_{ID}，输出用户的公钥 PK_{ID}。

4) 部分私钥提取算法 $(ID,PK_{ID},params)$。由 PKG 运行，输入用户的身份 ID、用户的公钥 PK_{ID}、系统参数 $params$，输出用户的部分私钥 s_{ID}。

5)时间密钥提取算法 $(ID,PK_{ID},params,t)$。由 PKG 运行，输入用户的身份 ID、用户的公钥 PK_{ID}、系统参数 $params$ 和当前时间 t，输出用户的时间密钥 $s_{ID,t}$。

6) 私钥提取($ID, x_{ID}, s_{ID}, s_{ID,t}$)。由用户运行，输入用户的身份 ID、秘密值 x_{ID}、部分私钥 s_{ID}、时间密钥 $s_{ID,t}$，输出用户的私钥 sk_{ID}。

7) 认证($ID, sk_{ID}, PK_{ID}, params$)。由用户运行，输入用户的身份 ID、用户私钥 sk_{ID}、用户公钥 PK_{ID} 和系统参数 $params$，生成请求消息 M。然后将 M 发给 AP。AP 验证消息 M 的有效性，如果有效，输出 Accept；否则，输出 Reject。

8) 撤销($ID, t, s_{ID,t}$)。由 PKG 运行，当用户 ID 的密钥泄露或服务到期时，停止为 ID 更新时间密钥 $s_{ID,t}$。

3.4 安全模型

本文协议涉及以下 3 类敌手。

1) 敌手 A_1。该敌手是外部敌手，他不知道系统主密钥，但可以替换任意合法用户的公钥以及从公共信道得到用户的时间密钥。

2) 敌手 A_2。这类敌手有诚实但是好奇的 PKG，他可以知道系统的主密钥，但是不能替换用户公钥。

3) 敌手 A_3。这类敌手是已经撤销的用户，他不知道系统主密钥和更新的时间密钥，但可以替换用户公钥。

协议的安全性由以下 3 个游戏表示。

游戏 1　挑战者 C 运行初始化算法，生成系统参数和主密钥。C 保留主密钥，发送系统参数给 A_1。A_1 可以进行询问。

1) 用户秘密值询问。A_1 发送一个用户的身份 ID，C 执行用户秘密值算法，然后将 x_{ID} 返回。

2) 用户公钥询问。A_1 询问身份为 ID 的用户公钥，C 执行公钥提取算法，然后将 PK_{ID} 返回。

3) 部分私钥询问。A_1 发送一个用户的身份 ID，C 执行部分私钥提取算法，然后将 s_{ID} 返回。

4) 时间密钥询问。A_1 询问身份为 ID 的用户在 t 时刻的时间密钥，C 执行时间密钥提取算法，然后将 $s_{ID,t}$ 返回。

5) 公钥替换询问。A_1 将身份为 ID 的用户公钥 PK_{ID} 替换成 PK'_{ID}。C 将记录该过程。

6) 认证询问。A_1 代表身份为 ID 的用户在公钥 PK_{ID} 和时间 t 下进行认证询问，C 执行认证算法得到认证消息 $\{X_i, Q_i\}$，然后将 $\{X_i, Q_i\}$ 返回给 A_1。

A_1 输出身份 ID^* 在 PK^*_{ID} 和 t^* 下的认证消息 $\{X_i^*, Q_i^*\}$。若满足以下条件，则 A_1 赢得游戏。

①A_1 没有执行过对 (ID^*, t^*) 的认证询问。

②A_1 没有提交过对 ID^* 的部分私钥询问。

③$\{X_i^*, Q_i^*\}$ 可以通过认证。

游戏 2　C 运行初始化算法，产生系统参数和系统主密钥，然后将参数和主密钥发送给 A_2。A_2 可以进行以下询问。

1) 用户秘密值询问。A_2 发送一个用户的身份 ID，C 执行秘密值提取算法，然后将 x_{ID} 返回。

2) 用户公钥询问。A_2 询问身份为 ID 的用户公钥，C 执行公钥提取算法，然后将 PK_{ID} 返回。

3) 认证询问。A_2 代表身份为 ID 的用户在公钥 PK_{ID} 和时间 t 下进行认证询问，C 执行认证算法得到认证消息 $\{X_i, Q_i\}$，然后将 $\{X_i, Q_i\}$ 返回。

A_2 输出身份 ID^* 在 PK^*_{ID} 和 t^* 下的认证消息 $\{X_i^*, Q_i^*\}$。若满足以下条件，则 A_2 赢得游戏。

①A_2 没有执行过对 (ID^*, t^*) 的认证询问。

②A_2 没有询问过对用户 ID^* 的秘密值询问。

③$\{X_i^*, Q_i^*\}$ 可以通过验证。

游戏 3　C 执行初始化算法，产生系统参数和系统主密钥。C 保留主密钥，但将参数发给 A_3。A_3 可以进行以下询问。

1) 时间密钥询问。A_3 询问身份为 ID 的用户在 t 时刻的时间密钥，C 执行时间密钥提取算法，然后将 $s_{ID,t}$ 返回。

2) 公钥替换询问。A_3 将身份为 ID 的用户公钥 PK_{ID} 替换成 PK'_{ID}。C 将记录下该过程。

3) 认证询问。A_3 代表身份为 ID 的用户在公钥 PK_{ID} 和时间 t 下进行认证询问，C 执行认证算法得到认证消息 $\{X_i, Q_i\}$，然后将 $\{X_i, Q_i\}$ 返回给 A_3。

A_3 输出身份 ID^* 在 PK^*_{ID} 和 t^* 下的认证消息 $\{X_i^*, Q_i^*\}$。若满足以下条件，则 A_3 赢得游戏。

①A_3 没执行 (ID^*, t^*) 的认证询问。

②A_3 没提交过对 (ID^*, t^*) 的时间密钥询问。

③$\{X_i^*, Q_i^*\}$ 可以通过验证。

定义 1　如果敌手 A_1、A_2 和 A_3 赢得游戏 1、游戏 2 和游戏 3 的概率都是可忽略的，那么认证协议是安全的。

4　本文的认证协议

为了满足安全性需求以及实现用户撤销，本文提出了一种新的高效可撤销的无证书远程匿名认证协议。协议包括 4 个阶段：初始化阶段、密钥生成阶段、认证阶段和撤销阶段。

4.1 初始化阶段

给定安全参数 λ，PKG 执行以下步骤。

1) 根据 2.1 节内容生成大素数 p、q 和 $\{F_p, E/F_p, G, P\}$，其中，G 的阶为 q。

2) PKG 随机选择 $s \in_R Z_q^*$，计算 $P_{\text{pub}} = sP$。维持一个身份时间列表 ITL，用于记录撤销用户的身份和时间，初始状态下 ITL 为空。定义散列函数 $h: \{0,1\}^* \times G^2 \to Z_q^*$、$h_1: \{0,1\}^* \times G^2 \times \{0,1\}^* \to Z_q^*$、$h_2: \{0,1\}^* \times G^2 \to Z_q^*$、$h_3: G^3 \times \{0,1\}^* \to Z_q^*$、$h_4: G \to \{0,1\}^l$、$h_5: G^4 \to \{0,1\}^*$。PKG 公布公开参数 $\{E/F_p, F_p, G, P, P_{\text{pub}}, h, h_1, h_2, h_3, h_4, h_5\}$，如图 3 所示。

4.2 密钥生成阶段

当 AP 提供服务之前，需要先执行以下的步骤向 PKG 注册。

1) AP 随机选择 $x_{\text{AP}} \in_R Z_q^*$，计算公钥 $PK_{\text{AP}} = x_{\text{AP}}P$。然后将 PK_{AP} 和其身份 ID_{AP} 发给 PKG。

2) PKG 收到 ID_{AP} 和 PK_{AP} 后，执行以下步骤。

①PKG 随机选择 $r_{\text{AP}} \in_R Z_q^*$，计算 $R_{\text{AP}} = r_{\text{AP}}P$，$a_{\text{AP}} = h(ID_{\text{AP}}, PK_{\text{AP}}, R_{\text{AP}})$，$s_{\text{AP}} = r_{\text{AP}} + a_{\text{AP}}s$。然后将 $(R_{\text{AP}}, s_{\text{AP}})$ 通过安全信道发送给 AP。AP 收到 $(R_{\text{AP}}, s_{\text{AP}})$ 后，计算 $a_{\text{AP}} = h(ID_{\text{AP}}, R_{\text{AP}}, PK_{\text{AP}})$，通过等式 $s_{\text{AP}}P = R_{\text{AP}} + a_{\text{AP}}P_{\text{pub}}$ 验证部分私钥的合法性。

②PKG 随机选择 $w_{\text{AP}} \in_R Z_q^*$，计算 $W_{\text{AP}} = w_{\text{AP}}P$，$b_{\text{AP}} = h_1(ID_{\text{AP}}, PK_{\text{AP}}, W_{\text{AP}}, t)$，$s_{\text{AP},t} = w_{\text{AP}} + b_{\text{AP}}s$，其中，$t$ 是系统初始化时间。最后将 $(W_{\text{AP}}, s_{\text{AP},t})$ 通过公共信道发送给 AP。AP 收到 $(W_{\text{AP}}, s_{\text{AP},t})$ 后，计算 $b_{\text{AP}} = h(ID_{\text{AP}}, PK_{\text{AP}}, t, W_{\text{AP}})$，通过等式 $s_{\text{AP},t}P = W_{\text{AP}} + b_{\text{AP}}P_{\text{pub}}$ 来验证时间密钥的合法性。

身份为 $ID_{\text{C}} \in \{0,1\}^*$ 的 C 随机选择 $x_{\text{C}} \in_R Z_q^*$，计算公钥 $PK_{\text{C}} = x_{\text{C}}P$。然后将 $\{ID_{\text{C}}, PK_{\text{C}}\}$ 发给 PKG。PKG 以相同的方式为 C 生成部分私钥 $s_{\text{C}} = r_{\text{C}} + a_{\text{C}}s$ 和时间密钥 $s_{\text{C},t} = w_{\text{C}} + b_{\text{C}}s$，并将 AP 的信息 $(ID_{\text{AP}}, R_{\text{AP}}, W_{\text{AP}}, PK_{\text{AP}})$ 发送给 C 保存。

最终，C 的私钥为 $(x_{\text{C}}, s_{\text{C}}, s_{\text{C},t})$，公钥为 PK_{C}。AP 的私钥为 $(x_{\text{AP}}, s_{\text{AP}}, s_{\text{AP},t})$，公钥为 PK_{AP}。具体过程如图 3 所示。

4.3 认证阶段

1) C 随机选择 $c_i \in_R Z_q^*$，计算 $X_i = c_iP$，$PK_{\text{AP}}^* = (PK_{\text{AP}} + R_{\text{AP}} + h(ID_{\text{AP}}, PK_{\text{AP}}, R_{\text{AP}})P_{\text{pub}} + W_{\text{AP}} + h(ID_{\text{AP}}, PK_{\text{AP}}, W_{\text{AP}}, t)P_{\text{pub}})$，$v_i = h_2(ID_{\text{C}}, X_i, X_i', t_{\text{C}})$，$l_i = h_3(ID_{\text{C}}, R_{\text{C}}, t_{\text{C}}, W_{\text{C}}, PK_{\text{C}})$，$\sigma_i = l_i(s_{\text{C}} + s_{\text{C},t} + x_{\text{C}}v_i) + c_i$，$X_i' = c_iPK_{\text{AP}}^*$，$Q_i = h_4(X_i') \oplus (ID_{\text{C}} \| \sigma_i \| R_{\text{C}} \| W_{\text{C}} \| PK_{\text{C}})$，其中，$t_{\text{C}}$ 是当前时间戳。然后将 $M = \{Q_i, X_i, t_{\text{C}}\}$ 发送给 AP。

2) 当 AP 收到 $\{Q_i, X_i, t_{\text{C}}\}$ 后，首先检测时间戳

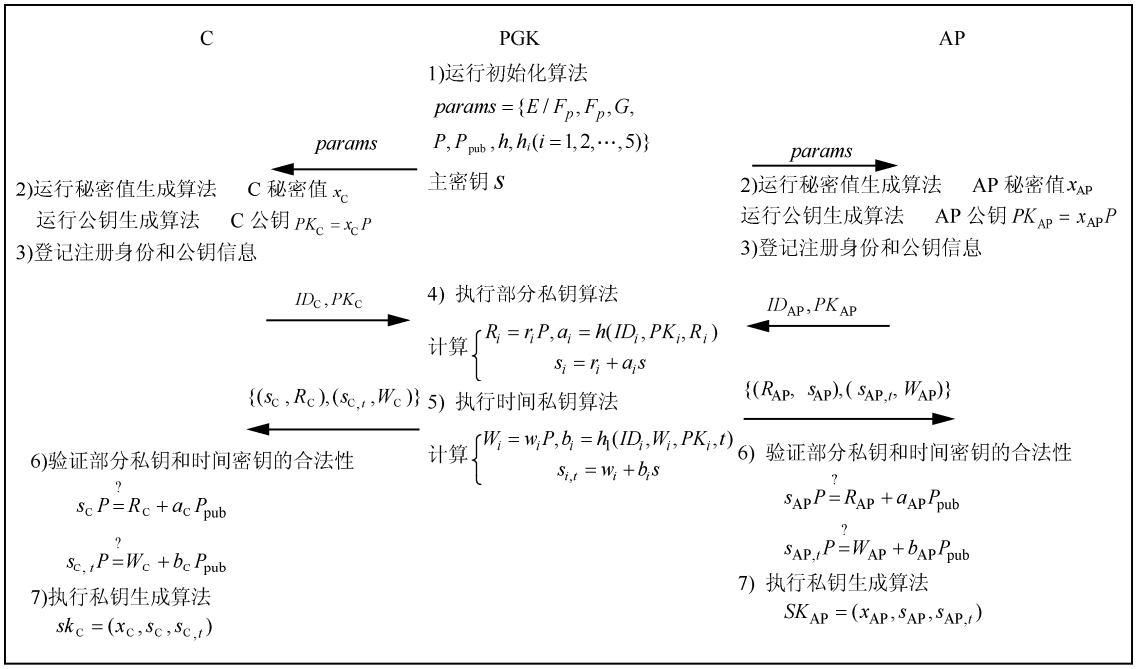


图 3 初始化和密钥生成阶段的具体过程

t_C 的有效性。如果有效，则 AP 计算 $X_i'=(x_{AP}+s_{AP}+s_{AP,t})X_i$，$(ID_C\|\sigma_i\|PK_C\|R_C\|W_C)=h_4(X_i')\oplus Q_i$，$a_C=h(ID_C,R_C,PK_C)$，$b_C=h_1(ID_C,t,\ PK_C,W_C)$，$v_i=h_2(ID_C,X_i,X_i',t_C)$，$l_i=h_3(ID_C,t_C,PK_C,R_C,W_C)$，然后 AP 验证 $\sigma_iP=l_i(R_C+W_C+a_CP_{pub}+b_CP_{pub}+v_i\cdot PK_C)+X_i$ 是否成立。如果不成立，则中止会话；否则，AP 随机选择 $d_i\in_R Z_q^*$，计算 $Y_i=d_iP$，$Y_i'=d_iX_i$，$sk=h_5(X_i,\ X_i',Y_i,Y_i')$ 以及 $MAC_{sk}(Y_i)$。最后将 $\{Y_i,MAC_{sk}(Y_i)\}$ 返回给 C。此外，AP 可以通过批认证验证多条请求消息的有效性。

3) C 收到 $\{Y_i,MAC_{sk}(Y_i)\}$，计算 $Y_i'=c_iY_i$，$sk=h_5(X_i,X_i',Y_i,Y_i')$。然后验证 $MAC_{sk}(Y_i)$ 的有效性，如果有效，则接受 sk 作为会话密钥；否则拒绝该 sk。具体认证过程如图 4 所示。

4.4　撤销阶段

当用户的服务到期或密钥泄露时，PKG 需要撤销该用户。PKG 将时间 t 更新为最新的撤销时间然后通过公共信道为未撤销的用户分发更新的时间密钥。PKG 维持一个列表 ITL，记录撤销用户身份和撤销时间。具体如表 1 所示。例如，在 t_2 时刻，PKG 检测到身份为 ID_{C_1} 的密钥泄露或服务到期，PKG 将 (ID_{C_1},t_1) 存储在 ITL 表中，然后为未撤销用户分发时刻为 t_2 的时间密钥。

表 1　　**撤销过程**

用户注册	ID_{C_1} 撤销	ID_{AP_1}撤销
(ID_{C_1},t_1)	(ID_{C_1},t_1)	(ID_{C_1},t_1)
⋮	⋮	⋮
(ID_{C_n},t_1)	(ID_{C_n},t_2)	(ID_{C_n},t_3)
(ID_{AP_1},t_1)	(ID_{AP_1},t_2)	(ID_{AP_1},t_2)
⋮	⋮	⋮
(ID_{AP_k},t_1)	(ID_{AP_k},t_2)	(ID_{AP_k},t_3)

5　安全性分析

5.1　安全性证明

引理 1　在随机预言模型下，如果 A_1 能在多项式时间内以不可忽略的优势 ε 攻破本文的协议，其中，A_1 最多进行 q_s 次认证询问、q_k 次部分私钥询问和 q_t 次时间密钥询问，则存在 S 可以以不可忽略的概率 $\varepsilon'\geqslant\frac{\varepsilon}{q_se}$ 解决 DL 问题。

证明　假定 A_1 是攻击者，给定 $\{P,aP\}$，构造算法 S，利用 S 解决 DL 问题，计算 a。

设 $P_{pub}=aP$，其中，a 是系统主密钥。S 维护列表 L、L_1、L_2、L_3、L_4、L_K、L_t、L_{PK} 分别用于存储 A_1 对 h、h_1、h_2、h_3、h_4、部分私钥、时间密钥和用户公钥询问的记录。初始状态下列表为空。A_1 可

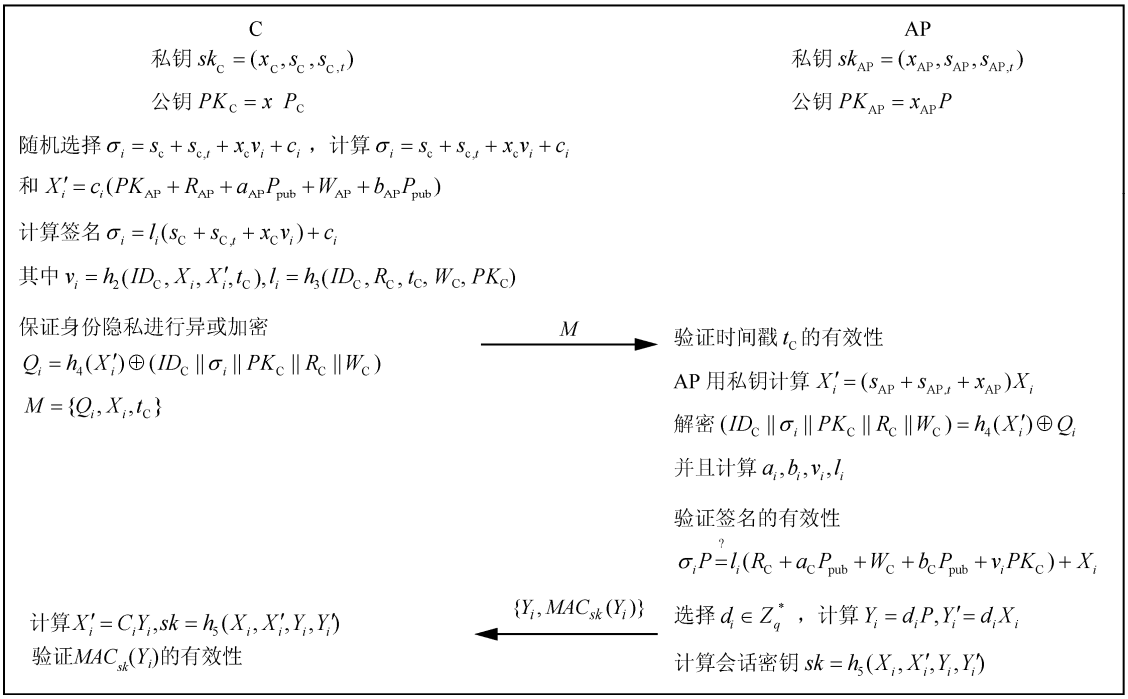


图 4　认证协议具体过程

以执行以下询问。

h 询问。收到 A_1 对 $\{ID_C, R_C, PK_C, a_C\}$ 的 h 询问后，S 进行以下操作。

1) 若表 L 存在 $\{ID_C, R_C, PK_C, a_C\}$，则返回 a_C 给 A_1。

2) 否则，S 随机选择 $a_C \in Z_q^*$，将 a_C 返回给 A_1 并添加 $\{ID_C, R_C, PK_C, a_C\}$ 到 L 中。

h_1 询问。收到 A_1 对 $\{ID_C, t, PK_C, W_C, b_C\}$ 的 h_1 询问后，S 进行以下操作。

1) 若列表 L_1 中存在 $\{ID_C, W_C, b_C, t, PK_C\}$，则返回 b_C 给 A_1。

2) 否则，S 随机选择 $b_C \in Z_q^*$，将 b_C 返回给 A_1 并添加 $\{ID_C, W_C, PK_C, t, b_C\}$ 到 L_1 中。

部分私钥询问。收到 A_1 对 $\{ID_C, PK_C\}$ 的部分私钥询问后，S 进行以下操作，其中，S 随机选择 ID^* 的概率为 θ。

1) 若 $ID_C = ID^*$，S 失败并终止模拟。

2) 否则，S 随机选择 $s_C, a_C \in Z_q^*$，计算 $R_C = s_C P - a_C P_{pub}$。将 (s_C, R_C) 返回给 A_1 并添加 $\{ID_C, PK_C, s_C, R_C\}$ 到 L_k 中。

时间密钥询问。收到 A_1 对 $\{ID_C, t, PK_C\}$ 的时间密钥询问后，S 执行以下操作。

1) 若表 L_t 中存在 $\{ID_C, PK_C, t, s_{C,t}, W_C\}$，则返回 $(s_{C,t}, W_C)$ 给 A_1。

2) 否则，S 随机选择 $s_{C,t}, b_C \in Z_q^*$，计算 $W_C = s_{C,t} P - b_C P_{pub}$。将 $\{s_{C,t}, W_C\}$ 返回给 A_1 并添加 $\{ID_C, PK_C, s_{C,t}, t, W_C\}$ 到 L_t。

用户秘密值询问。收到 A_1 对 ID_C 的秘密值询问后，S 检索 ID_C 的公钥询问列表 x_C，然后将 x_C 返回给 A_1。

用户公钥询问。收到 A_1 对 ID_C 的公钥询问后，S 进行以下操作。

1) 若 $ID_C = ID^*$，选择 $x_C, r_C \in Z_q^*$，设置 $PK_C = x_C P$，$R_C = r_C P$。然后将 PK_C 返回给 A_1 并添加 $\{ID_C, PK_C, x_C\}$ 到 L_{PK} 中。

2) 否则，S 随机选择 $x_C \in Z_q^*$，计算 $PK_C = x_C P$。将 PK_C 返回给 A_1 并添加 $\{ID_C, PK_C, x_C\}$ 到 L_{PK} 中。

公钥替换询问。收到 A_1 对 PK_C 的公钥替换询问后，S 从表 L_{PK} 中检索 $\{ID_C, PK_C, x_C\}$，令 $PK_C = PK_C'$，并将 $\{ID_C, PK_C, \perp\}$ 添加到表 L_{PK} 中。

h_1 询问。收到 A_1 对 $\{ID_C, X_i, X_i', t_C\}$ 的 h_2 询问后，S 进行以下操作。

1) 当表 L_2 中有 $\{ID_C, X_i, X_i', t_C, v_i\}$，则返回 v_i 给 A_1。

2) 否则，S 随机选择 $v_i \in_R Z_q^*$，返回 v_i 并将 $\{ID_C, X_i, X_i', t_C, v_i\}$ 加入 L_2 中。

h_3 询问。收到 A_1 对 $\{ID_C, R_C, W_C, t_C, PK_C\}$ 的 h_3 询问后，S 进行以下操作。

1) 当表 L_3 中有 $\{ID_C, R_C, W_C, PK_C, t_C, l_i\}$，则返回 l_i 给 A_1。

2) 否则，S 选择 $l_i \in Z_q^*$，返回 l_i 给 A_1 并将 $\{ID_C, R_C, W_C, PK_C, t_C, l_i\}$ 加入 L_3 中。

h_4 询问。收到 A_1 对 X_i' 的 h_4 询问后，S 进行以下操作。

1) 当表 L_3 中有 $\{h_4, X_i'\}$，则返回 h_4 给 A_1。

2) 否则 S 随机选择 $h_4 \in \{0,1\}^l$，返回 l_i 给 $\{ID_C, R_C, W_C, t_C\}$ 并将 $\{h_4, X_i'\}$ 加入 L_4 中。

认证询问。收到 A_1 对 $\{ID_C, PK_C, t\}$ 的认证询问后，S 进行以下操作。

1) 若 $(ID_C, t) \neq (ID^*, t^*)$ 并且公钥未被替换，S 选择 $c_i \in Z_q^*$，计算 $X_i = c_i P$，$X_i' = c_i PK_{AP}^*$，$\sigma_i = l_i(s_C + s_{C,t} + x_C v_i) + c_i$ 和 $Q_i = h_4(X_i') \oplus (ID_C \| \sigma_i \| PK_C \| R_C \| W_C)$ 并将 $\{X_i, Q_i\}$ 返回给 A_1。

2) 若 $(ID_C, t) = (ID^*, t^*)$ 或公钥已经被替换，S 失败并终止模拟。

最后 A_1 输出 $\{ID_C^*, PK_C^*, t^*\}$ 的认证消息 $\{X_i^*, Q_i^*\}$。

A_1 选择 $\sigma_i^*, v_i \in Z_q^*$，计算 $X_i^* = \sigma_i^* P - l_i(R_C + a_C P_{pub} + s_{C,t} P) - v_i PK_C$，$Q_i^* = h_4(X_i^*) \oplus (ID^* \| \sigma_i^* \| PK_C \| R_C \| W_C)$。然后将认证消息 $\{X_i^*, Q_i^*\}$ 返回给 S。S 收到 $\{X_i^*, Q_i^*\}$ 后，计算 $X_i'^* = (s_{AP} + x_{AP}) X_i$，解密 Q_i^* 得到 $(ID^* \| \sigma_i^* \| PK_C \| R_C \| W_C)$。其中，签名 $\{X_i^*, \sigma_i^*\}$ 满足式(1)

$$\sigma_i^* P = l_i(R_C + a_C P_{pub} + s_{C,t} P + v_i PK_C) + X_i^* \quad (1)$$

S 根据分叉引理[17]选择不同的 h 可以得到另一个合法认证消息 $\{X_i^*, \hat{Q}_i^*\}$，并且签名 $\{X_i^*, \hat{\sigma}_i^*\}$ 满足式(2)

$$\hat{\sigma}_i^* P = l_i(R_C + \hat{a}_C P_{pub} + s_{C,t} P + v_i PK_C) + X_i^* \quad (2)$$

根据式(1)和式(2)，可以推出

$$\begin{aligned}(\sigma_i^*-\hat{\sigma}_i^*)P&=\sigma_i^*P-\hat{\sigma}_i^*P\\&=l_i(R_{\mathrm{C}}+a_{\mathrm{C}}P_{\mathrm{pub}}+s_{\mathrm{C},t}P+v_iPK_{\mathrm{C}})+X_i^*-\\&\quad l_i(R_{\mathrm{C}}+\hat{a}_{\mathrm{C}}P_{\mathrm{pub}}+s_{\mathrm{C},t}P+v_iPK_{\mathrm{C}})-X_i^*\\&=l_i(a_{\mathrm{C}}-\hat{a}_{\mathrm{C}})aP\end{aligned}$$

最后，S 输出 $(\sigma_i^*-\hat{\sigma}_i^*)\,[l_i(a_C-\hat{a}_C)]^{-1}$ 作为 DL 问题的结果。这与 DL 问题的困难性相悖，所以本文的协议是安全的。

引理 2　在随机预言模型下，如果 A_2 能在多项式时间内以不可忽略的优势 ε 攻破本文的认证协议，其中，A_2 最多进行 q_s 次认证询问，q_k 次部分私钥询问和 q_t 次时间密钥询问，则存在 S 可以以不可忽略的概率 $\varepsilon'\geqslant\dfrac{\varepsilon}{q_s e}$ 解决 DL 问题。

证明　假定 A_2 是攻击者，给定 $\{P,aP\}$，构造算法 S，利用 S 解决 DL 问题，计算 a。

S 设 $P_{\mathrm{pub}}=sP$，其中，s 是系统主密钥。A_2 知道系统主密钥并且 A_2 不允许执行公钥替换询问。其中，h、h_1、h_2、h_3、h_4 询问可参见引理 1。

用户公钥询问。收到 A_2 对 ID_{C} 的公钥询问后，S 进行以下操作。

1) 若 $ID_{\mathrm{C}}=ID^*$，S 选择 $a_{\mathrm{C}},b_{\mathrm{C}}\in Z_q^*$，计算 $R_{\mathrm{C}}=s_{\mathrm{C}}P-a_{\mathrm{C}}P_{\mathrm{pub}}$，$W_{\mathrm{C}}=s_{\mathrm{C},t}\ P-b_{\mathrm{C}}P_{\mathrm{pub}}$，设置 $PK_{\mathrm{C}}=aP$。然后返回 PK_{C} 给 A_2 并添加 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},\perp\}$ 到表 L_{PK} 中。

2) 否则，S 选择 $x_{\mathrm{C}},a_{\mathrm{C}},b_{\mathrm{C}}\in Z_q^*$，计算 $R_{\mathrm{C}}=s_{\mathrm{C}}P-a_{\mathrm{C}}P_{\mathrm{pub}}$，$W_{\mathrm{C}}=s_{\mathrm{C},t}P-b_{\mathrm{C}}P_{\mathrm{pub}}$，设置 $PK_{\mathrm{C}}=x_{\mathrm{C}}P$。然后将 PK_{C} 返回给 A_2 并添加 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},x_{\mathrm{C}}\}$ 到表 L_{PK} 中。

用户秘密值询问。收到 A_2 对 ID_{C} 的秘密值询问后，S 进行以下操作。

1) 若 $ID_{\mathrm{C}}=ID^*$，S 失败并终止模拟。

2) 否则，S 检索 ID_{C} 的公钥询问列表 x_{C}，然后将 x_{C} 返回给 A_2。

认证询问。收到 A_2 对 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},t\}$ 的认证询问后，S 进行以下操作。

1) 若 $(ID_{\mathrm{C}},t)\neq(ID^*,t^*)$，随机选择 $c_i\in Z_q^*$，S 计算 $X_i=c_iP$，$X_i'=c_iPK_{\mathrm{AP}}^*$，$\sigma_i=l_i(s_{\mathrm{C}}+s_{\mathrm{C},t}+x_{\mathrm{C}}v_i)+c_i$ 和 $Q_i=h_4(X_i')\oplus(ID_{\mathrm{C}}\,\|\,\sigma_i\,\|\,PK_{\mathrm{C}}\,\|\,R_{\mathrm{C}}\,\|\,W_{\mathrm{C}})$ 并将 $\{X_i,Q_i\}$ 返回给 A_2。

2) 若 $(ID_{\mathrm{C}},t)=(ID^*,t^*)$，$S$ 失败并终止模拟。

最后 A_2 输出 $\{ID_{\mathrm{C}}^*,PK_{\mathrm{C}}^*,t^*\}$ 的认证消息 $\{X_i^*,Q_i^*\}$。

A_2 选择 $X_i^*=\sigma_i^*P-s_cP-s_{c,t}P-v_iPK_c$，计算 $X_i^*=\sigma_i^*P-l_i(v_iPK_{\mathrm{C}}+s_{\mathrm{C}}P+s_{\mathrm{C},t}P)$，$Q_i^*=h_4(X_i'^*)\oplus(ID^*\,\|\,\sigma_i^*\,\|\,PK_{\mathrm{C}}\,\|\,R_{\mathrm{C}}\,\|\,W_{\mathrm{C}})$ 并将 $\{X_i^*,Q_i^*\}$ 返回给 S。S 收到 $\{X_i^*,Q_i^*\}$ 后，计算 $X_i'^*=(s_{\mathrm{AP}}+x_{\mathrm{AP}})X_i$，解密 Q_i^* 得到 $(ID^*\,\|\,\sigma_i^*\,\|\,PK_{\mathrm{C}}\,\|\,R_{\mathrm{C}}\,\|\,W_{\mathrm{C}})$。其中，签名 $\{X_i^*,\sigma_i^*\}$ 满足式(3)

$$\sigma_i^*P=l_i(s_{\mathrm{C}}P+s_{\mathrm{C},t}P+v_iPK_{\mathrm{C}})+X_i^* \tag{3}$$

S 根据分叉引理[17]选择不同的 h_2 可以得到另一个认证消息 $\{X_i^*,\hat{Q}_i^*\}$。其中，签名 $\{X_i^*,\hat{\sigma}_i^*\}$ 满足式(4)

$$\hat{\sigma}_i^*P=l_i(s_{\mathrm{C}}P+s_{\mathrm{C},t}P+\hat{v}_iPK_{\mathrm{C}})+X_i^* \tag{4}$$

根据式(3)和式(4)，可以推出

$$\begin{aligned}\sigma_i^*P-\hat{\sigma}_i^*P&=l_i(s_{\mathrm{C}}P+s_{\mathrm{C},t}P+v_iPK_{\mathrm{C}})+\\&\quad X_i^*-l_i(s_{\mathrm{C}}P+s_{\mathrm{C},t}P+\hat{v}_iPK_{\mathrm{C}})-X_i^*\\&=l_i(v_i-\hat{v}_i)aP\end{aligned}$$

最后，S 输出 $(\sigma^*-\hat{\sigma}^*)\,[l_i(v_i-\hat{v}_i)]^{-1}$ 作为 DL 问题的结果。这与 DL 问题的困难性相悖，所以本文的协议是安全的。

引理 3　在随机预言模型下，如果 A_3 能在多项式时间内以不可忽略的优势 ε 攻破认证协议，其中，A_3 最多进行 q_s 次认证询问，q_k 次部分私钥询问和 q_t 次时间密钥询问，则存在 S 可以以不可忽略的概率 $\varepsilon'\geqslant\dfrac{\varepsilon}{q_s e}$ 解决 DL 问题。

证明　假定 A_3 是攻击者，给定 $\{P,aP\}$，构造算法 S，利用 S 解决 DL 问题，计算 a。

S 设 $P_{\mathrm{pub}}=aP$，其中，a 是系统主密钥。A_3 是已经撤销的用户，知道秘密值和部分私钥。A_3 执行的 h、h_1、h_2、h_3、h_4 以及秘密值，公钥替换询问可参见引理 1。

部分私钥询问。收到 A_3 对 $\{ID_{\mathrm{C}},PK_{\mathrm{C}}\}$ 的部分私钥询问后，S 进行以下操作。

1) 当表 L_t 中有 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},R_{\mathrm{C}},s_{\mathrm{C}}\}$，则返回 $(s_{\mathrm{C}},R_{\mathrm{C}})$ 给 A_3。

2) 否则，S 随机选择 $s_{\mathrm{C}},a_{\mathrm{C}}\in Z_q^*$，计算 $R_{\mathrm{C}}=s_{\mathrm{C}}P-a_{\mathrm{C}}P_{\mathrm{pub}}$。将 (s_C,R_C) 返回给 A_3 并添加 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},s_{\mathrm{C}},R_{\mathrm{C}}\}$ 到 L_k 中。

时间密钥询问。收到 A_3 对 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},t\}$ 的时间密钥询问后，S 进行以下操作。

1) 若 $(ID_{\mathrm{C}},t)\neq(ID^{*},t^{*})$，$S$ 随机选取 $s_{\mathrm{C},t}$，$b_{\mathrm{C}}\in Z_q^{*}$，计算 $W_{\mathrm{C}}=s_{\mathrm{C},t}P-b_{\mathrm{C}}P_{\mathrm{pub}}$，返回 $\{s_{\mathrm{C},t},W_{\mathrm{C}}\}$ 给 A_3，并添加 $\{ID_{\mathrm{C}},t,s_{\mathrm{C},t},W_{\mathrm{C}},PK_{\mathrm{C}}\}$ 到 L_t 中。

2) 若 $(ID_{\mathrm{C}},t)=(ID^{*},t^{*})$，$A_3$ 失败并终止模拟。

用户公钥询问。收到 A_3 对 ID_{C} 的公钥询问后，S 进行以下操作。

1) 若 $ID_{\mathrm{C}}=ID^{*}$，随机选择 $w_{\mathrm{C}}\in Z_q^{*}$，计算 $W_{\mathrm{C}}=w_{\mathrm{C}}P$，$PK_{\mathrm{C}}=x_{\mathrm{C}}P$。然后将公钥 PK_{C} 返回给 A_3 并添加 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},x_{\mathrm{C}}\}$ 到表 L_{PK} 中。

2) 否则，S 随机选择 $s_{\mathrm{C},t},b_{\mathrm{C}}\in Z_q^{*}$，计算 $W_{\mathrm{C}}=s_{\mathrm{C},t}P-b_{\mathrm{C}}P_{\mathrm{pub}}$，$PK_{\mathrm{C}}=x_{\mathrm{C}}P$。然后，将公钥 PK_{C} 返回给 A_3 并添加 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},x_{\mathrm{C}}\}$ 到表 L_{PK} 中。

认证询问。收到 A_3 对 $\{ID_{\mathrm{C}},PK_{\mathrm{C}},t\}$ 的认证询问后，S 进行以下操作。

1) 若 $(ID_{\mathrm{C}},t)\neq(ID^{*},t^{*})$ 并且公钥未被替换，选择 $c_i\in Z_q^{*}$，S 计算 $X_i=c_iP$，$X_i'=c_iPK_{\mathrm{AP}}^{*}$，$\sigma_i=l_i(s_C+s_{C,t}+x_Cv_i)+c_i$ 和 $Q_i=h_4(X_i')\oplus(ID_{\mathrm{C}}\|\sigma_i\|PK_{\mathrm{C}}\|R_{\mathrm{C}}\|W_{\mathrm{C}})$ 并将 $\{X_i,Q_i\}$ 返回给 A_3。

2) 若 $(ID_{\mathrm{C}},t)=(ID^{*},t^{*})$ 或公钥已经被替换，S 失败并终止模拟。

最后，A_3 输出 $\{ID_{\mathrm{C}}^{*},PK_{\mathrm{C}}^{*},t^{*}\}$ 的认证消息 $\{X_i^{*},Q_i^{*}\}$。

A_3 选择 $X_i^{*}=\sigma_i^{*}P-s_{\mathrm{C}}P-(W_{\mathrm{C}}+b_{\mathrm{C}}P_{\mathrm{pub}})-v_iPK_{\mathrm{C}}$，计算 $X_i^{*}=\sigma_i^{*}P-l_i\ (s_{\mathrm{C}}P+v_iPK_{\mathrm{C}}+b_{\mathrm{C}}P_{\mathrm{pub}}+W_{\mathrm{C}})$ 以及 $Q_i^{*}=h_4(X_i'^{*})\oplus(ID^{*}\|\sigma_i^{*}\|PK_{\mathrm{C}}\|R_{\mathrm{C}}\|W_{\mathrm{C}})$。然后将 $\{X_i^{*},Q_i^{*}\}$ 返回给 S。S 收到 $\{X_i^{*},Q_i^{*}\}$ 后，计算 $X_i'^{*}=(s_{\mathrm{AP}}+x_{\mathrm{AP}})X_i$，解密 Q_i^{*} 后得到 $ID^{*}\|\sigma_i^{*}\|PK_{\mathrm{C}}\|R_{\mathrm{C}}\|W_{\mathrm{C}}$。其中，签名 $\{X_i^{*},\sigma_i^{*}\}$ 满足式(5)

$$\sigma_i^{*}P=l_i(s_{\mathrm{C}}P+W_{\mathrm{C}}+b_{\mathrm{C}}P_{\mathrm{pub}}+v_iPK_{\mathrm{C}})+X_i^{*} \tag{5}$$

S 根据分叉引理[17]选择不同的 h_1 可以得到另一个合法认证消息 $\{X_i^{*},\hat{Q}_i^{*}\}$，并且签名 $\{X_i^{*},\hat{\sigma}_i^{*}\}$ 满足式(6)

$$\hat{\sigma}_i^{*}P=l_i(s_{\mathrm{C}}P+W_{\mathrm{C}}+\hat{b}_{\mathrm{C}}P_{\mathrm{pub}}+v_iPK_{\mathrm{C}})+X_i^{*} \tag{6}$$

根据式(5)和式(6)，可以推出

$$\begin{aligned}(\sigma_i^{*}-\hat{\sigma}_i^{*})P&=l_i(s_{\mathrm{C}}P+W_{\mathrm{C}}+b_{\mathrm{C}}P_{\mathrm{pub}}+v_iPK_{\mathrm{C}})+\\&\quad X^{*}-l_i(s_{\mathrm{C}}P+W_{\mathrm{C}}+\hat{b}_{\mathrm{C}}P_{\mathrm{pub}}+v_iPK_{\mathrm{C}})-X^{*}\\&=l_i(b_{\mathrm{C}}-\hat{b}_{\mathrm{C}})aP\end{aligned}$$

最后，S 输出 $(\sigma_i^{*}-\hat{\sigma}_i^{*})[l_i(b_{\mathrm{C}}-\hat{b}_{\mathrm{C}})]^{-1}$ 作为 DL 问题的结果。这与 DL 问题困难性相悖，所以本文的协议是安全的。

5.2 其他安全性分析

下面的分析证实本文协议也满足客户匿名、相互认证、不可链接、会话密钥安全、前向安全和可撤销等安全性需求。

1) 客户匿名性。C 的身份包含在消息 M 中，其中，$Q_i=h_4(X_i')\oplus(ID_{\mathrm{C}}\|\sigma_i\|R_{\mathrm{C}}\|W_{\mathrm{C}}\|PK_{\mathrm{C}})$。敌手想要得到客户身份需要计算 $X_i'=c_iPK_{\mathrm{AP}}^{*}$，即敌手需要解决 CDH 问题。而 CDH 问题是难解的，所以本文的协议满足客户匿名性。

2) 相互认证性。在前面的分析中可以得出只有合法的 C 和 AP 可以生成合法请求消息 $\{Q_i,X_i,t_{\mathrm{C}}\}$ 和应答 $\{MAC_{sk}(Y_i),Y_i\}$。因此，C 和 AP 可以通过验证消息的有效性来确定对方是否合法。所以本文的协议满足相互认证性。

3) 不可链接性。假设 C 发送的 2 条请求消息为 $\{Q_1,X_1,t_{\mathrm{C}_1}\}$ 和 $\{Q_2,X_2,t_{\mathrm{C}_2}\}$，其中，$X_i=c_iP$，$Q_i=h_4(X_i')\oplus(ID_{\mathrm{C}}\|\sigma_i\|R_{\mathrm{C}}\|W_{\mathrm{C}}\|PK_{\mathrm{C}})$，$X_i'=c_iPK_{\mathrm{AP}}^{*}$。由于在不同的请求消息中，$c_i$ 是随机数，因此，敌手不能知道这 2 条消息是由同一个 C 发送的。所以本文的协议满足不可链接性。

4) 会话密钥安全性。相互认证之后，C 和 AP 将建立会话密钥 $sk=h_5(X_i,X_i',Y_i,Y_i')$，其中，$X_i=c_iP$，$X_i'=c_iPK_{\mathrm{AP}}^{*}$，$Y_i=d_iP$，$Y_i'=d_iX_i$。如果敌手想要伪造会话密钥，需要解决 CDH 问题。而 CDH 问题是难解的，所以本文协议能够提供会话密钥安全性。

5) 前向安全性。在协议的执行过程中，C 和 AP 可以生成会话密钥 $sk=h_5(X_i,X_i',Y_i,Y_i')$。即使敌手知道 C 和 AP 的长期私钥，计算会话密钥还需要从 $X_i=c_iP$，$Y_i=d_iP$ 中计算出 c_id_iP，即要解决 CDH 问题。而 CDH 问题是难解的，所以本文的协议满足前向安全性。

6) 可撤销性。当用户的密钥泄露或服务到期时，PKG 需要撤销该用户。此时 PKG 将为未撤销的用户更新时间密钥 $s_{\mathrm{C},t}/s_{\mathrm{AP},t}$，而撤销用户的时间密钥将不更新，所以本文协议可撤销性。

6 功能和性能分析

6.1 功能比较分析

本节将本文协议与文献[12,13]的协议进行功能

对比。表 2 中√表示能满足该性质，×表示不能满足该性质。可见本文协议和文献[13]中的协议满足所有的常见安全性需求，而文献[12]中协议未考虑到用户撤销问题。

表 2　　功能对比

安全性需求	文献[12]协议	文献[13]协议	本文协议
用户匿名性	√	√	√
相互认证性	√	√	√
不可链接性	√	√	√
会话密钥安全性	√	√	√
前向安全性	√	√	√
可撤销性	×	√	√

6.2　C 端及 AP 端性能分析

本文协议中C端在Inter® Core i7 CPU 3.6 GHZ处理器，内存为 512 MB，操作系统为 Win7 上模拟，AP 端在 Inter® Core i5CPU 2.4 GHz 处理器，内存为 4 GB，操作系统为 Win10 OS 上模拟，并使用 JPBC 库[18]量化密码学操作时间。在模拟实验中采用超奇异曲线 $E/F_P: y^2 = x^3 + x$，其中，阶 q 是 160 bit 的 Solonas 素数，G_1 中的元素为 512 bit，假定协议中使用的身份信息和时间戳均为 32 bit。此外，对称加密/解密操作、消息认证码以及普通散列函数操作的时间较短[19]，可以忽略不计。

6.2.1　计算代价分析

通过模拟实验结果取 20 次平均值得到 C 和 AP 的计算代价。根据模拟实验结果，给出图 5 和图 6 的代价对比。图 5 中给出本文协议中 C 的计算代价随着 AP 数量增加的关系，对应多位专家会诊等现实情况，图 6 中给出本文协议中 AP 端计算代价随着 C 数量增加的关系。本文的协议基于椭圆曲线，没有使用高代价的双线性对以及 map-to-point 散列操作。由图 5 和图 6 可以看出，与文献[12]和文献[13]相比，C 端及 AP 端的计算代价有了大幅降低。

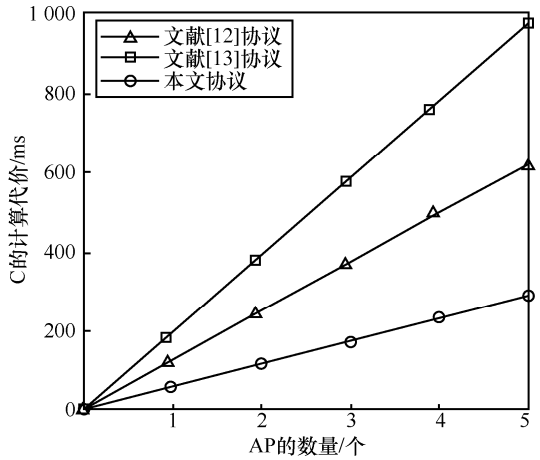


图 5　C 端计算代价与 AP 端数量的关系

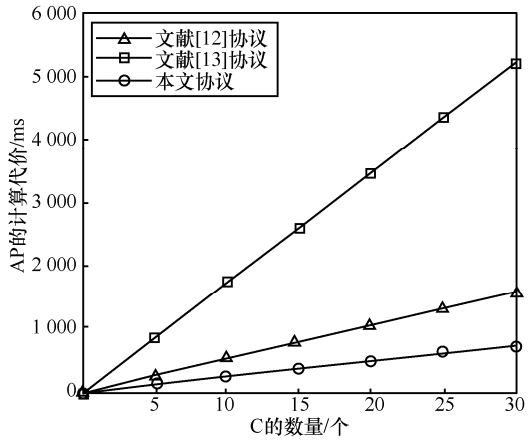


图 6　AP 端计算代价与 C 端数量的关系

6.2.2　存储代价分析

通过模拟实验选定的参数 q、G，可以计算得到协议的存储代价。

在文献[12]的协议中，C 存储 $2m+3$ 个 G 中的元素和 m 个身份信息，其中，m 表示 AP 的数量。所以 C 端的存储代价为 $160\times(2m+3)+32m=(480+352m)$ bit；AP 存储 3 个 G 中的元素，所以 AP 端的存储代价为 $160\times3=480$ bit。

在文献[13]的协议中，WBAN 的用户个数为 $n=2^a$ 个，C 存储 $2a+3$ 个 G_1 中的元素和一个随机数，所以 C 端的存储代价为 $512\times(2a+3)+160=(1\,024a+1\,696)$ bit。AP 端存储 $2a+3$ 个 G_1 的元素和一个随机数，所以 AP 端存储代价为 $512\times(2a+3)+160=(1\,024a+1\,696)$ bit。

在本文协议中，C 存储 $3m+5$ 个 G 中的元素和 m 个身份信息，其中，m 表示 AP 的数量。所以 C 端的存储代价为 $160\times(3m+5)+32m=(512m+800)$ bit；AP 端存储 5 个 G 中的元素，则 AP 端的存储代价为 $160\times5=800$ bit。具体比较如表 3 所示，在实际应用中 m 远远小于 n。由于本文协议实现了用户撤销，需要多存储额外的时间密钥，所以代价比文献[12]要稍高。但与文献[13]对比，本文协议的存储代价大大降低。

表 3 存储代价对比

协议	存储代价/bit	
	C 端	AP 端
文献[12]协议	480+352 m	480
文献[13]协议	1 024 a +1 696	1 024 a +1 696
本文协议	800+512 m	800

6.2.3 通信代价分析

通过模拟实验选定的参数 q、G，可以计算得到协议的通信代价。

在文献[12]的协议中，C 发送的消息包括 4 个 G 中的元素，一个身份信息和一个时间戳。AP 发送的消息包括一个 G 中元素和一个 MAC 码。所以协议的通信代价为 160×5+32+32+160=1 024 bit。

在文献[13]的协议中，C 发送的消息包括 8 个 G_1 中的元素，一个身份信息和一个时间戳。AP 发送的消息包括一个 G_1 中元素和一个 MAC 码。所以协议的通信代价为 512×9+160+32+32=4 832 bit。

在本文的协议中，C 发送的消息包括 5 个 G 中元素，一个身份信息和一个时间戳，AP 发送的消息包括一个 G 中元素和一个 MAC 码。所以协议的通信代价为 160×6+ 32+32+160=1 184 bit。表 4 给出了详细的通信代价比较，本文协议比文献[12]通信代价稍高，因为在传输过程中需要发送额外的参数，但是本文考虑了用户撤销的问题，代价稍高是可以接受的。

表 4 通信代价比较

协议	通信代价/bit
文献[12]协议	1 024
文献[13]协议	4 832
本文协议	1 184

6.3 PKG 性能分析

文献[13]的协议中使用 KUNode 算法进行用户撤销，PKG 计算和分发时间密钥的代价是 n 和 r 的函数，其中，n 是用户个数，r 是撤销用户的个数。当 $r \leqslant \frac{n}{2}$ 时，PKG 的密钥更新代价随着用户而对数增加；当 $r > \frac{n}{2}$，PKG 的密钥更新代价随着用户而线性增加。虽然这种方案可以降低 PKG 的更新代价，但是会导致 C 端存储大量树形结构中的内容，存储代价较大。在本文协议中，PKG 的撤销代价是随着用户个数线性增加的。由表 5 可以看出，在撤销用户较少的情况下，本文协议中 PKG 的更新代价相对于 KUNode 算法会较高，但是由表 5 可以看出本文协议大大减少了 C 端的存储代价。而 PKG 的资源比较充足，增加 PKG 的代价是可行的。所以本文协议更加适用于 WBAN。

表 5 PKG 撤销代价对比

协议	复杂度		
	$r=0$	$1 \leqslant r \leqslant \frac{n}{2}$	$\frac{n}{2} < r \leqslant n$
文献[13]协议	$O(1)$	$O\left(r\log\left(\frac{n}{r}\right)\right)$	$O(n-r)$
本文协议	$O(1)$	$O(n-r)$	$O(n-r)$

7 结束语

本文基于时间密钥和椭圆曲线提出了可撤销的无证书远程匿名认证协议，实验结果表明本文协议大大降低了用户端的计算代价和存储代价。经过安全性证明以及详细的功能分析说明本文协议是安全有效的，更适用于资源受限的无线体域网。

参考文献：

[1] ZIMMERMAN T G. Personal area networks: near-field intra body communications[J]. IBM System Journal, 1996, 35(3/4):609-617.

[2] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(24):770-772.

[3] LI M, YU S, LOU W, et al. Group device pairing based secure sensor association and key management for body area networks[C]// Conference on Information Communications. 2010:2651-2659.

[4] LI M, YU S, GUTTMAN J D, et al. Secure ad hoc trust initialization and key management in wireless body area networks[J]. ACM Transactions on Sensor Networks, 2013, 9(2):1-35.

[5] YANG J H, CHANG C C. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem[J]. Computer Security, 2009, 28 (3-4):138-143.

[6] HE D, CHEN J, HU J. An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security[J]. Information Fusion, 2012, 13(3):223-230.

[7] HE D, ZEADALLY S, KUMAR N, et al. Anonymous authentication for wireless body area networks with provable security[J]. IEEE System Journal, 2016, (99):1-12.

[8] SHAMIR A. Identity-based cryptosystems and signature schemes[M]// Advances in Cryptology (Lecture Notes in Computer Science). Springer-Verlag, 1984, 196:47-53.

[9] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//International Conference on the Theory and Application of

Cryptology and Information Security. 2003:452-473.

[10] LIU J, ZHANG Z, SUN R, et al. An efficient certificateless remote anonymous authentication scheme for wireless body area networks[C]//IEEE International Conference on Communications. 2012:3404-3408.

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

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

[13] XIONG H, QIN Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(7):1442-1455.

[14] SEO J H, EMURA K. Revocable identity-based cryptosystem revisited: security models and constructions[M]. IEEE Press, 2014.

[15] TSAI T T, TSENG Y M. Revocable certificateless public key encryption [J]. IEEE Systems Journal, 2015, 9(3):824-833.

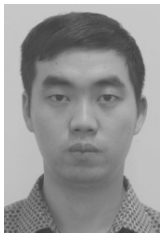
[16] CILARDO A, COPPOLINO L, MAZZOCCA N, et al. Elliptic curve cryptography engineering[J]. Proceedings of the IEEE, 2006, 94(2): 395-406.

[17] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[C]// ACM Conference on Computer and Communications Security. 2006:390-399.

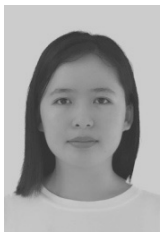
[18] CARO A D, IOVINO V. jPBC: Java pairing based cryptography[C]// Computers and Communications. 2011:850-855.

[19] CHATTERJEE S, DAS A, SING J. An enhanced access control scheme in wireless sensor networks[J]. Ad-Hoc Sensor Wireless Network, 2014, 21(1-2):121-149.

[作者简介]



张顺（1982-），男，安徽安庆人，安徽大学副教授、硕士生导师，主要研究方向为信息安全、信息计算复杂性。



范鸿丽（1993-），女，安徽滁州人，安徽大学硕士生，主要研究方向为网络与信息安全。

仲红（1965-），女，安徽固镇人，安徽大学教授、博士生导师，主要研究方向为无线传感网、安全多方计算、私有信息保护。

田苗苗（1987-），男，安徽阜阳人，安徽大学副教授、硕士生导师，主要研究方向为密码学和信息安全。