脑机接口技术中安全高效的属性基访问控制

屠袁飞*①②③ 杨 庚①② 袁冯杰③
①(南京邮电大学通信与信息工程学院 南京 210003)
②(江苏省无线传感网高技术研究重点实验室 南京 210003)
③(南京工业大学计算机科学与技术学院 南京 211800)

摘 要：随着脑机接口技术(Brain-Computer Interface, BCI)在新兴医疗健康监测领域的广泛应用，其受到的安全威胁越来越多，导致其隐私保护问题受到了关注。该文针对 BCI 应用中的隐私保护问题提出一种通信模型，并为其设计了一种基于密文策略的属性基(Ciphertext-Policy Attribute Based Encryption, CP-ABE)访问控制方案，利用代理重加密技术实现细粒度的属性撤销。经分析表明，方案有效地解决了 BCI 模型中敏感数据的隐私保护问题，并且在能量损耗及通信计算开销等性能评估中表现优异。

关键词：脑机接口技术；隐私保护；访问控制方案；属性撤销；代理重加密
中图分类号： TP393; TP309 **文献标识码**： A **文章编号**：1009-5896(2017)10-2495-09
DOI: 10.11999/JEIT161362

Secure and Efficient Attribute Based Access Control for Brain-computer Interface

TU Yuanfei①②③ YANG Geng①② YUAN Fengjie③
①(*College of Telecommunications and Information Engineering*, *Nanjing University of Post and Telecommunication*, *Nanjing* 210003, *China*)
②(*Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks*, *Nanjing* 210003, *China*)
③(*College of Computer Science and Technology*, *Nanjing Tech University*, *Nanjing* 211800, *China*)

Abstract: Brain-Computer Interface (BCI) are expected to play a major role in field of medical-health monitoring in near future. Unfortunately, an increasing number of attacks to BCI applications underline the existence of security and privacy related issues, which gains tremendous attention amongst researchers. In this paper, a communication architecture is proposed for BCI applications, and an access control scheme is designed by employing Ciphertext-Policy Attribute Based Encryption (CP-ABE). The proposed scheme supports fully fine-grained attribute revocation by proxy re-encryption. The proposed scheme can efficiently and feasibly reduce the challenges of privacy preservation, and it works excellent in energy consumption and communication/computation overhead.

Key words: Brain-Computer Interface (BCI); Privacy preservation; Access control scheme; Attribute revocation; Proxy re-encryption

1 引言

随着人类在脑神经科学方面研究的突破，脑机接口技术(Brain Computer Interface, BCI)的开发及应用成为一股风潮[1–3]。BCI 通过可穿戴式的脑电(ElectroEncephaloGram, EEG)传感器[4,5]采集脑波信号并经智能手机通过 4G 网络传输到分析平台进行存储、分析、共享[6]。这一系统中包含了大量的隐私数据，然而 BCI 制造商基本忽略了用户敏感信息泄露的问题[7]，加上无线网易被入侵，手机遗失等特性，隐私保护问题突出。

在 2012 年 USENIX 安全会议上，Martinovic 等人[8]首次发布了针对 BCI 用户的恶意攻击软件，软件分析 EEG 响应信号获取病人的隐私信息。攻击者甚至可提取用户的记忆，性格以及行为取向等信息[9]，并对人脑产生干扰，进一步控制用户的行为[10]。近年来，美国明确提出了保护用户的医疗信息法

收稿日期：2016-12-13；改回日期：2017-07-11；网络出版：2017-08-14
*通信作者：屠袁飞 yuanfeitu@163.com
基金项目：国家自然科学基金(61572263, 61272084)，江苏省高校自然科学研究重大项目(11KJA520002)，高等学校博士学科点专项科研基金(20113223110003)，中国博士后科学基金(2015M581794)，江苏省博士后科研资助计划(1501023C)，南京邮电大学校级科研基金(NY214127)
Foundation Items: The National Natural Science Foundation of China (61572263, 61272084), The Natural Science Foundation of the Jiangsu Province Higher Education Institutions of China (11KJA520002), The Specialized Research Fund for the Doctoral Program of Higher Education (20113223110003), China Postdoctoral Science Foundation (2015M581794), Jiangsu Province Planned Projects for Postdoctoral Research Funds (1501023C), NUPTSF (NY214127)

律[11]，坚决抵制对用户医疗信息的恶意攻击行为[12]。

对此有学者提出通过跨学科合作，开发阻止信息泄露的工具，实现隐私保护，其中加密是目前应用比较普遍的手段。文献[13,14]为 BCI 的安全与隐私保护问题提出了一种匿名方案，方案在存储和传输神经信号之前对信号进行处理，除去特定 BCI 命令外的所有用户信息，以防止原始神经信号的泄露。但是该方案仅保留了必要的神经信息，造成后续分析中，不能对用户产生的数据与其包含的信息进行深入挖掘。文献[15,16]直接利用传感器对体感信号进行加密，将生理属性作为密钥，持有相同密钥的用户可解密数据，但当攻击者得到病人的生理信号时，即可直接解密该信号加密的数据，造成隐私泄露的问题。文献[17]提出了一种基于身份的加密方案，保护了传感器数据的隐私，同时能够在轻量级设备上运行，但是方案没有提出具体的访问控制模型。

从密码学角度分析，如何管理对称加密密钥的安全是必须解决的问题。非对称加密安全性更好，但其加解密时间长、速度慢、计算复杂度高。此外，仅靠加密手段无法实现灵活的访问控制功能，对用户身份的动态变化适应性不够。通过认证进入系统的用户，面对系统的全部资源，也可能会破坏其他不可访问资源的隐私。

为了适应开放网络环境下资源保护所面临的细粒度控制策略、安全等需求，人们提出了基于属性的访问控制(Attibute-Based Access Conrol, ABAC)[18,19]。用属性描述的策略可以表达基于属性的逻辑语义，灵活地描述访问控制策略[20]。基于属性的访问控制研究的两个重要方面为基于密文策略(CP-ABE)和基于密钥策略(KP-ABE)的控制[21]。在 CP-ABE 方案中，密文中嵌入了访问控制结构，即加密之后就确定了哪些用户能够对它进行解密而不需要借助可信服务器来实现这种控制。

随着时间的推移，用户属性会发生变化，相应的访问策略也要有变化，属性撤销成为 ABE 必须解决的问题。目前大多数方案主要关注如何支持表述能力更为丰富的解密策略，而没有特别地考虑属性撤销问题。这就意味着，在实际应用中，系统需要周期性地进行重新加密数据及分发新密钥的工作，系统负荷也随之增加。

本文利用基于属性的加密算法能够有效实现细粒度非交互访问控制[22,23]的特点，为 BCI 系统提出了安全高效的访问控制方案，本方案支持任意的线性秘密共享方案(Linear Secret-Sharing Schemes, LSSS)访问结构，有效地控制了用户权限，保护了数据隐私。采用代理重加密技术实现了细粒度的支持属性级别的撤销，访问策略更加灵活。利用智能手机存储密文，对属性变化的密文部分进行重加密，降低了传感器的运算量。最后，分析了方案的安全性与性能开销，并给出了仿真结果。

2 预备知识及系统模型

2.1 预备知识

2.1.1 双线性映射 设 G_1 和 G_2 是两个 p 阶循环群，其中 p 为一大素数。设 P 为 G_1 的生成元，定义双线性映射 $e: G_1 \times G_1 \to G_2$ 满足如下条件：

(1)双线性：对任意的 $P, Q \in G_1, a, b \in Z_p$，满足 $e(P^a, Q^b) = e(P,Q)^{ab}$，其中 $Z_p = \{0,1,\cdots,p-1\}$。

(2)非退化性：$e(P,P) \neq 1$。

(3)可计算性：对任意 $P, Q \in G_1, a, b \in Z_p$，存在一个有效的多项式时间算法计算出 $e(P,Q)$。

2.1.2 线性秘密共享方案 一个基于成员集 P 的秘密共享方案 Π 在 Z_p 上是线性的需要满足以下两个条件：

(1)每个成员所分得秘密的一部分构成一个 Z_p 上的矩阵。

(2) Π 中存在一个 $l \times (n+1)$ 秘密共享矩阵 $\boldsymbol{M}$。对于 $i = 1,2,\cdots,l$，$\boldsymbol{M}$ 的第 i 行表示第 i 个成员 $x_i \in P$。设一个列向量 $\boldsymbol{V} = (s, r_1, r_2, \cdots, r_n)$，其中 $s \in Z_p$ 是待分享的秘密，是随机的，则 $\boldsymbol{M} \cdot \boldsymbol{V}$ 把秘密 s 根据 Π 分成 l 个部分。$(\boldsymbol{M} \cdot \boldsymbol{V})_i$ 属于成员 x_i。

2.1.3 线性重构 Π 是访问结构 A 上的一个 LSSS 方案。设 $S \in A$ 是任意一个授权集，$I = \{i : x_i \in S\} \subset \{1,2,\cdots,l\}$，那么可以在多项式时间内找出这样的常数集 $\{\omega_i \in Z_p\}_{i \in I}$，使得 $\sum_{i \in I} \omega_i \cdot (\boldsymbol{M} \cdot v)_i = s$。

2.2 系统模型

如图 1 所示，系统包含 4 个实体：授权中心(Key Generation Center, KGC)，EEG 传感器(EEG Sensor, ES)，智能手机(Data Sink, DS)以及数据用户(Data Consumers, DC)。

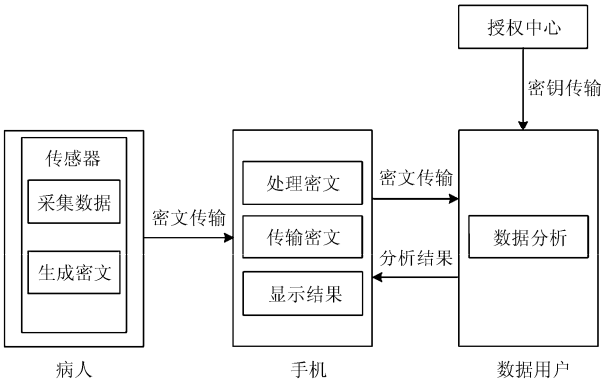

图 1 BCI 系统模型

KGC 执行系统初始化程序，生成公钥及主密钥，管理系统中的属性。主密钥被秘密的保存在KGC 中，公钥则被保存在传感器中。

发生属性撤销时，KGC生成新的参数，建立与手机的安全通信连接，将新参数发送到手机，由手机完成对密文的更新。

EEG传感器采集用户的脑波信号，根据访问策略对数据进行加密，之后再把密文发送到手机。

智能手机，即数据接收器，对加密过的病人脑波信号进行存储、更新、转发，其自身也没有访问原始数据的权限，即使攻击者获得该手机，也只能获得密文数据。此外，手机不需做实时、在线的访问控制，降低了运算量。

数据用户一般为医生、护士等。用户向KGC声明其所拥有的属性，获得属性私钥。如果数据用户的属性满足密文中所定义的访问策略，则用户可通过该私钥获得访问原始数据的权限。

3　访问控制模型

访问控制通过限制主体对客体的访问权限，明确用户可访问的资源范围以及相应操作，保证客体被正确合理地访问，维护资源拥有者的利益。图1所示模型中，脑电数据会存储在手机及数据分析平台上，数据属主无法直接对数据用户提供访问服务，而传统的访问控制方法对这一情境并不适用，使资源的访问控制成为需要解决的问题。因此本文在文献[24]的基于属性的加密算法基础上，提出了一种面向BCI的保护用户隐私的访问控制模型。

在实际应用中，病人通过这一在线服务模型，应能创建、控制其 EEG 数据，与多方用户进行分享，并可持续地控制其 EEG 数据访问权限。通过基于属性的访问控制方法，即使病人不知道数据用户的具体身份信息，仍可以用一系列的属性对其进行描述，选择可访问的用户，如家庭成员，亲密的朋友，医生，护士，医学研究人员，保险公司人员，甚至可以进一步细化到身份证号、工号等。

如图 2 所示，某病人根据此访问策略对其 EEG 数据加密，那么医院 A 的神经科主任医师将可以获得访问 EEG 数据的权限，而大学 A 的心理学助教则无法对该密文进行解密。病人根据其需要添加各种属性，构建访问策略，从而实现灵活、细粒度的访问控制。

3.1 方案构造

算法 1　系统初始化 Setup($\boldsymbol{U}$)

系统初始化算法输入系统属性集 U，设 G_1，G_2 是两个阶为大素数 p 的乘法循环群，P 是 G_1 的一个

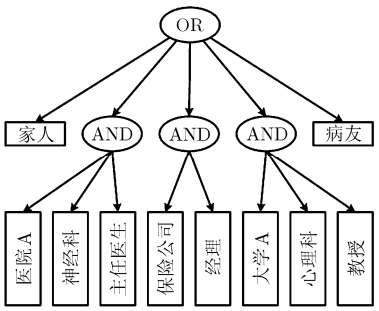

图 2 访问策略

生成元，定义 $e: G_1 \times G_1 \to G_2$ 是一个双线性映射。KGC 在群 G_1 中选取与属性集中 u 个属性对应的随机元素 $Q_1, Q_2, \cdots, Q_u \in G_1$，此外，随机选取 $\alpha, a \in Z_p$，属性值 $\mathrm{Att}_1, \mathrm{Att}_2, \cdots, \mathrm{Att}_u \in Z_p$，生成系统公钥为

$$\mathrm{PK} := < P, e(P,P)^{\alpha}, aP, Q_1, Q_2, \cdots, Q_u, T_1 = \mathrm{Att}_1 P, \cdots, T_u > \tag{1}$$

主密钥为

$$\mathrm{MK} := < \alpha, \mathrm{Att}_1, \mathrm{Att}_2, \cdots, \mathrm{Att}_u > \tag{2}$$

算法 2　加密算法 Encrypt(PK,$(\boldsymbol{M},\boldsymbol{\rho})$,$\boldsymbol{K}$)

加密算法输入系统公钥 PK, LSSS 矩阵访问结构 $(\boldsymbol{M},\rho)$ 以及消息 K。

令 $\boldsymbol{M}$ 为一个 $l \times n$ 阶的矩阵，l 为用户属性数，n 为访问策略中的属性数，函数 ρ 将 $\boldsymbol{M}$ 中的每一行映射到一个用户属性。在 Z_p 上随机选择一个矢量 $\boldsymbol{v} = (s, y_2, y_3, \cdots, y_n)$ 用于分享加密元素 s，对 $i = 1, 2, \cdots, l$，计算 $\lambda_i := \boldsymbol{v} \cdot \boldsymbol{M}_i$，其中 $\boldsymbol{M}_i$ 为 $\boldsymbol{M}$ 的第 i 行，再随机选取 $r_1, r_2, \cdots, r_l \in Z_p$，得到密文如式(3)：

$$\begin{aligned} \mathrm{CT} &:= < C, C', (C_1, D_1), (C_2, D_2), \cdots, (C_l, D_l) > \\ &= < Ke(P,P)^{\alpha s}, sP, \left(\lambda_1(aP) - r_1 Q_{\rho(1)}, r_1 T_{\rho(1)}\right), \\ &\quad \cdots, \left(\lambda_l(aP) - r_l Q_{\rho(l)}, r_l T_{\rho(l)}\right) > \end{aligned} \tag{3}$$

算法 3　私钥生成算法 KeyGen(MK,$\boldsymbol{S}$)

私钥生成算法输入主密钥 MK 和一个用户属性列表 S, KGC 向该用户发放与属性相关的私钥。KGC 随机选取 $t_{\mathrm{ID}} \in Z_p$，算法输出 t_{ID} 和属性私钥 SK，生成的 SK 为

$$\mathrm{SK} := < K, L, \forall x \in S \quad K_x >= < \alpha P + t_{\mathrm{ID}}(aP), t_{\mathrm{ID}} P, \forall x \in S \left(t_{\mathrm{ID}} / \mathrm{Att}_x\right) Q_x > \tag{4}$$

算法 4　解密算法 Decrypt(SK,CT)

解密算法以属性私钥 SK 以及密文 CT 为输入，拥有 SK 的解密者试图解密 CT，假设用户的属性列表 S 满足访问结构 (M,ρ)，则存在 $\{\omega_i \in Z_p\}_{i \in I}$ 使得 $\sum_{i \in I} \omega_i \lambda_i = s$，其中 $I = \{i : \rho(i) \in s\}$。

解密算法首先计算：

$$\frac{e(C',K)}{\prod_{i\in I}\left(e(C_i,L)e\left(D_i,K_{\rho(i)}\right)\right)^{\omega_i}}=\frac{e(P,P)^{\alpha s}e(P,P)^{ast_{\mathrm{ID}}}}{\prod_{i\in I}\left(e(P,P)^{ta\lambda_i\omega_i}\right)}=e(P,P)^{\alpha s}$$

再计算输出明文：

$$K=C/e(P,P)^{\alpha s} \tag{5}$$

算法 5　密钥更新算法 KeyUpdate(MK,γ)

密钥更新算法以 MK 以及一组待更新属性集合 γ 为输入。对任意 $x\in\gamma$，KGC 随机选取 $\mathrm{Att}_x^{'}\in Z_p$ 作为新的属性密钥，计算

$$T_x^{'}:=\mathrm{Att}_x^{'}P,\ rk_{x\to x'}:=\mathrm{Att}_{x'}/\mathrm{Att}_x \tag{6}$$

用 $\mathrm{Att}_x^{'}$ 替代主密钥部件中的各个 Att_x，用 $T_x^{'}$ 替代公钥部件中的 T_x。算法输出重定义的主密钥 MK′，公钥 PK′，以及代理重加密密钥(PRE Keys)。

$$rk:=\{x,rk_x\}_{x\in\gamma} \tag{7}$$

算法 6　重加密算法 Re Enc($y(=\rho(i)),D_i$, $\mathbf{RKL}_y$)

重加密算法以一个待更新的属性 $y(=\rho(i))$，密文部件 D_i 和一个代理重加密列表 RKL_y 为输入，算法首先由 KGC 检查属性 y 的版本号，如果属性 y 有最新的版本号，算法输出 $\perp$ 并退出，否则定义 $\mathrm{Att}_{y(n)}$ 为最新的属性 y 的属性密钥，计算

$$rk_{y\to y(n)}:=rk_{y\leftrightarrow y'}\cdot rk_{y'\leftrightarrow y''},\cdots,rk_{y^{(n-1)}\leftrightarrow y^{(n)}}=\mathrm{Att}_{y(n)}/\mathrm{Att}_y \tag{8}$$

之后输出重加密的密文部件：

$$D_i^{'}:=rk_{y\leftrightarrow y(n)}\cdot D_i=\left(\mathrm{Att}_{y(n)}/\mathrm{Att}_y\right)r_i\mathrm{Att}_yP=r_i\mathrm{Att}_{y(n)}P \tag{9}$$

算法 7　私钥更新算法 Re KeyGen($w,\boldsymbol{K}_{w,\mathrm{ID}}$, $\mathbf{RKL}_w$)

该算法输入更新的属性 w，属性私钥部件 K_w 以及代理重加密列表 RKL_w，输出更新的属性私钥部件 $K_w^{'}$。算法首先检查属性 w 的版本号，如果属性 w 有最新的版本号，算法输出符号 $\perp$ 并退出，否则定义 $\mathrm{Att}_{w(n)}$ 为属性 w 的最新的属性私钥，计算：

$$rk_{w\to w(n)}:=rk_{w\leftrightarrow w'}\cdot rk_{w'\leftrightarrow w''},\cdots,rk_{w^{(n-1)}\leftrightarrow w^{(n)}}=\mathrm{Att}_{w(n)}/\mathrm{Att}_w \tag{10}$$

算法输出更新的属性私钥部件：

$$K_w^{'}:=rk_{w\leftrightarrow w(n)}^{-1}\cdot K_w=\left(\mathrm{Att}_w/\mathrm{Att}_{w(n)}\right)\cdot\left(t_{\mathrm{ID}}/\mathrm{Att}_w\right)Q_w=\left(t_{\mathrm{ID}}/\mathrm{Att}_{w(n)}\right)Q_w \tag{11}$$

3.2 用户读取数据

因为 ABE 算法本身的复杂性问题，并不适合对大型文件进行加密，因此本文采用混合加密的方式，首先利用对称加密算法(如 AES128)对 EEG 数据进行加密，得到会话密钥 K，再对 K 采用本文中的 ABE 算法进行加密，得到密钥的密文。数据存储格式如图 3 所示。

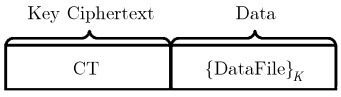

图 3 数据文件的密文格式

一个拥有属性集 S 的用户按如下步骤获取明文：

步骤 1　EEG 传感器从密钥空间中随机选取一个会话密钥 K，利用 AES 算法 AES(K,D)加密 EEG 信号 D；

步骤 2　定义该文件的访问结构；

步骤 3　EEG 传感器调用本文中的加密算法 2 加密上述会话密钥 K，得到密钥密文 CT，再按照图 3 的存储格式发送文件至手机。其中 EEG → DS 表示由传感器至手机的数据传输。

$$(\mathrm{Algorithm2}(K),\mathrm{AES}(K,D))\big|_{\mathrm{EEG}\to\mathrm{DS}} \tag{12}$$

步骤 4　用户向 KGC 声明其所拥有的属性，根据算法 3 获得属性私钥；

步骤 5　用户从手机获取加密数据，利用算法 4 得到会话密钥 K；

步骤 6　用户利用会话密钥 K 解密 AES(K,D) 得到原始EEG信号 D。

3.3 用户属性撤销时的通信

在发生属性撤销的情况下，KGC 需要执行密钥更新算法，保存主密钥 MK′ 和重加密密钥 rk，并将公钥 PK′ 经手机发送给 EEG 传感器，替换原有公钥。再根据重加密算法计算出 $rk_{y\to y^{(n)}}$，由手机将此组件与原密文对应组件相乘，输出重加密的密文部件，完成密文的更新。本文提出一种简单且安全的身份证明方案，以确保 KGC 与手机及传感器间的通信安全。

在这一过程中，EEG 传感器根据访问策略对访问令牌 K_1 加密，KGC 解密该密文，将获得的数据做哈希运算后再发回到 EEG 传感器进行比对认证，如果认证通过，则 EEG 传感器选取新的访问令牌对 KGC 进行第 2 次挑战，如果第 2 次挑战通过，那么 KGC 的身份就得到确认，在传感器和 KGC 之间可以建立安全的通信连接。

认证过程分为 3 个阶段：初始化阶段、通信建立阶段以及通信阶段，以下将详细描述 3 阶段的过程。

3.3.1 初始化阶段

步骤 1　KGC 利用算法 1 发布 PK，并且为属性拥有者分配相应的属性，比如医生、护士。

步骤 2　KGC 为相应的医生和护士分别发布其属性私钥，如 SK_D, SK_N。

步骤 3　EEG 传感器在为病人佩戴之前先存储公钥 PK。

3.3.2 通信建立阶段

步骤 1　传感器随机选取一个访问标记 K_1，利用算法 2 加密 $K_{\mathrm{Tdate}}=K_1\,||\,\mathrm{datetime}$，并将加密后的标记发送到手机。手机存储此访问标记，在 KGC 提出访问请求时将其发送。

$$\left(\mathrm{Algorithm2}\left(K_{\mathrm{Tdate}}\right),\mathrm{Hash}\left(K_{\mathrm{Tdate}}\right)\right)\Big|_{\mathrm{EEG}\to\mathrm{DS}} \tag{13}$$

Hash(•)表示发送端与接收端协议预先约定的哈希函数。

步骤 2　传感器定时更新访问标记 K_{Tdate}。

步骤 3　KGC 获取(Algorithm2(K_{Tdate}))后，通过算法 4 解密密文，并做哈希运算，再发回手机，供传感器读取验证：$H'=H(K_{\mathrm{Tdate}})\big|_{\mathrm{KGC}\to\mathrm{DS}}$。

步骤 4　传感器读取手机信息后，比较 H' 与 H 是否相等。若相等，则重新生成访问标记 $K_1^{'}$，利用算法 2 以相同的访问结构对 $K_{\mathrm{Tdate}}^{'}=K_1^{'}\|\mathrm{datetime}$ 进行加密，再将其发送到手机覆盖原访问标记，由 KGC 读取进行 2 次验证。

$$\left(\mathrm{Algorithm2}\left(K_{\mathrm{Tdate}}^{'}\right),\mathrm{Hash}\left(K_{\mathrm{Tdate}}^{'}\right)\right)\Big|_{\mathrm{EEG}\to\mathrm{DS}} \tag{14}$$

步骤 5　KGC 解密 $\left(\mathrm{Algorithm2}\left(K_{\mathrm{Tdate}}^{'}\right)\right)$，然后将得到的访问标记的哈希值 $H'=H\left(K_1^{'}\|\mathrm{datetime}\right)$ 发送回手机。

$$H'=H\left(K_1^{'}\|\mathrm{datetime}\right)\Big|_{\mathrm{KGC}\to\mathrm{DS}} \tag{15}$$

步骤 6　传感器读取手机，再次验证 H' 与 H 是否相等，如果验证通过，KGC 和手机便可将标记 $K_1^{'}$ 作为会话密钥进行安全的加密通信。

3.3.3 通信阶段

步骤 1　KGC 将更新后的公钥 $\mathrm{PK}', rk_{y\to y(n)}$ 用标记 $K_1^{'}$ 加密后发送到手机。

$$\left(\mathrm{AES}\left(K_1^{'},\mathrm{PK}'\|rk_{y\to y(n)}\right),\right.$$
$$\left.\mathrm{Hash}\left(\mathrm{PK}'\|rk_{y\to y(n)}\right)\right)_{\mathrm{KGC}\to\mathrm{DS}} \tag{16}$$

步骤 2　传感器读取手机，解密消息得到 $\mathrm{PK}', rk_{y\to y(n)}$，然后比较 $\left(H'=\mathrm{Hash}\left(\mathrm{PK}'\|rk_{y\to y(n)}\right)\right)$ 是否与 H 相等，如果相等，则证明消息的完整性。

步骤 3　传感器用 PK' 更新原有公钥，并将 $rk_{y\to y(n)}$ 发送到手机，由其更新密文。

3.4 会话密钥的有效期

本方案利用 CP-ABE 算法对会话密钥进行加密，如果用户属性符合访问策略，则能获得会话密钥。在实际使用中，为保证通信的安全，会话密钥在使用一段时间后就应被撤销。会话密钥的有效期越短，系统的安全性越高，但是系统开销也会增大。

4 方案分析

4.1 安全性分析

4.1.1 数据机密性　本方案中，数据文件的机密性取决于对称加密算法(AES)，而对称加密算法的机密性则主要取决于对称密钥 K 的安全性。密钥 K 的加密采用了基于属性的加密算法，该算法已被证明是安全的，未认证用户(如攻击者)的属性集不满足访问策略，因此无法正确解密获得 K，从而不能访问数据文件。

本方案中即使手机参与了重加密，它也不能解开密文，因为手机只被授权去利用其获得的密钥与密文组件进行乘法操作，该密钥并没有与属性集相关，因此手机也无法解开密文。

4.1.2 抗合谋攻击　基于属性的加密算法最大的挑战是防止合谋用户的攻击。在 CP-ABE 中，秘密共享值 s 嵌入在密文中。为了解开密文，用户或者合谋攻击者需要将 $e(P,P)^{\alpha s}$ 恢复出来。为了恢复出 $e(P,P)^{\alpha s}$，合谋攻击者必须利用密文中的组件 C_l，D_l和其他合谋用户的私钥组件 L 和 K_i作相应的双线性配对运算。但是，每一个用户的私钥都通过一个随机数 t_{ID} 唯一生成，每个用户的 t_{ID} 不同，因此即使用户合谋，$e(P,P)^{\alpha s}$ 的值也不会被恢复。只有当该用户具有的属性满足访问策略时 $e(P,P)^{\alpha s}$ 值才会被恢复。

4.1.3 两次身份认证　当 KGC 申请与手机进行通信时，传感器会随机选择一个标记进行加密，KGC 需要解密该标记，证明其身份合法。在第 1 次认证成功后，传感器再次随机生成一个访问标记对 KGC 进行 2 次身份认证。新的访问标记将覆盖手机中原访问标记，令攻击者没有足够的时间破解，保证会话的安全。

4.2 性能分析

本节对提出的算法进行了定量的性能研究。研究中主要关注密文长度、通信开销以及传输过程中产生的能量损耗。

4.2.1 密文长度　从数据用户与数据接收器之间的通讯协议来看，当用户第 1 次访问数据接收器时，需要利用式(12)获取会话密钥 K，根据式(3)和式(12)，可以计算出密文总长度为

$$\text{Size}=\left|\text{Algorithm2}(K)\right|=|C|+|C'|+2\left(\left|C_1\right|+\cdots+\left|C_l\right|\right)=(2l+2)|p| \quad (17)$$

在实际应用场景中，为达到足够的访问属性数目与较低的计算开销，令访问属性数 $l=10$。

式(17)中的每个参数长度是可变的，本方案的评估中，双线性映射 e 采用基于椭圆曲线上的 Tate 对，椭圆曲线定义在有限域 F_p 上，G_1 和 G_2 的阶 p 是一个 20 Byte 的素数。为了达到 1024 bit RSA 的安全等级，p 应为一个 64 Byte 的素数，其中 G_2 是一个定义在有限域 $F_{p^2}^*$ 上的乘法群的 p 阶子群。

设 p 为有限域 $F_{p^3}^*$ 上长度为 42.5 Byte 的素数，以及有限域 $F_{p^6}^*$ 上长度为 20 Byte 的素数。因此，式(17)计算出的总密文长度可表示为 $22|p|$ Byte，大小范围为 440 Byte 到 1408 Byte。

信道建立后，在下次会话生成之间的通信，由于用户拥有了会话密钥，其通信密文长度可表示为：

$$\text{Size}=\left|\text{AES}(K,D)\right|$$

其长度为 16 Byte。

同理根据式(3)和式(14)可计算出授权中心与手机之间通信时的密文长度如式(18)：

$$\begin{aligned}\text{Size}&=\left|\text{Algorithm2}\left(K'_{\text{Tdate}}\right)\right|+\left|\text{Hash}\left(K'_{\text{Tdate}}\right)\right|\\&=|C|+|C'|+2\left(\left|C_1\right|+\cdots+\left|C_l\right|\right)+\left|\text{Hash}\left(K'_{\text{Tdate}}\right)\right|=(2l+2)|p|+12\end{aligned} \quad (18)$$

按照相同的分析方法，从式(18)可以计算出总密文长度为(22|p|+12) Byte，大小范围为 452～1420 Byte。

数据用户成功建立链接之后，密文的长度为

$$\text{Size}=\left|\text{AES}\left(K'_1,\text{PK}'\|rk_{y\to y(n)}\right)\right|+\left|\text{Hash}\left(\text{PK}'\|rk_{y\to y(n)}\right)\right|$$

其大小等于 32 Byte。

表 1 可以看出，为了建立安全的通信连接，本方案会形成一个较大的密文长度，但当连接建立之后，数据用户和传感器之间的通信密文长度会大大缩短。由于密文长度直接决定了通信能量损耗与计算开销，因此在通信相对频繁时，本方案较短的密文长度能够保证更低的能量损耗与更小的计算开销。

表 1 密文长度

方案	加密(Byte)	解密
数据用户-手机	$22\|p\|$	1
授权中心-手机	$44\|p\|+24$	1
数据用户-手机	16	1
授权中心-手机	32	1

4.2.2 通信能量损耗 利用文献[25]中的方法评估计算本文方案所产生的能量损耗，使用无线传感器 MICA2DOT 节点中的射频芯片 CC1100 作为用户与数据接收器之间的无线通信模块，其工作在发送模式和接收模式时，分别发送和接收 1 Byte 所消耗的能量为 28.6 μJ 和 59.2 μJ。

本方案中，数据用户与数据接收器建立连接的消息总长度为 $22|p|$ Byte，一次数据传输所产生的总能量损耗(包括发送消息和接收消息)为

$$22\mid p\mid\times(28.6+59.2)\ (\mu\text{J})=1.93|p|\ (\text{mJ})$$

连接建立之后，消息长度为 16 Byte，产生的能量损耗为：

$$(16\times(28.6+59.5))\ (\mu\text{J})=1.40\ (\text{mJ})$$

当有 N 次数据传输时，产生的总能量损耗为：

$$(1.93|p|+1.40\times(N-1))\ (\text{mJ})$$

另一方面，授权中心与数据接收器之间的通信的密文长度为(22|p|+12) Byte，所产生的能量损耗为

$$\begin{aligned}&2\times(22\mid p\mid+12)\times(28.6+59.2)\ (\mu\text{J})\\&=(3.86\mid p\mid+2.11)\ (\text{mJ})\end{aligned}$$

用户身份认证后所产生的能量损耗为

$$32\times(28.6+59.2)\ (\mu\text{J})=2.81\ (\text{mJ})$$

当有 N 次数据传输时，所产生的总能量损耗为

$$\begin{aligned}&(2.81\times(N-1)+3.86\mid p\mid+2.11)\ (\text{mJ})\\&=(3.86\mid p\mid+2.81N-0.7)\ (\text{mJ})\end{aligned}$$

能量损耗与数据传输次数关系如图 4 所示，从图中能看出能量损耗与数据传输次数成线性关系，同时与安全等级成正相关。

表 2 展示了本文的方案和其他基准方案的能量损耗比较。

从表 2 分析得出，在相同的无线通信模型中，

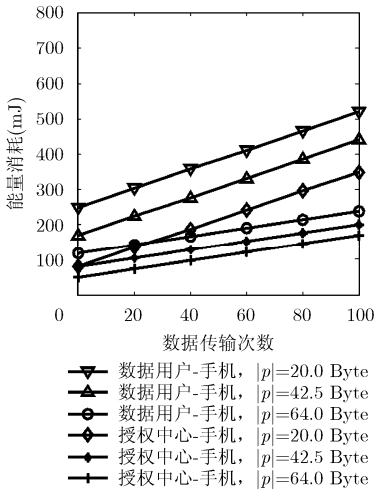

图 4 能量损耗与数据传输次数关系图

表 2 通信能量损耗

方案(Byte)	能量消耗(mJ)
数据用户-手机，$\|p\|$=20	$1.40N$+37.2
数据用户-手机，$\|p\|$=42.5	$1.40N$+80.63
数据用户-手机，$\|p\|$=64	$1.40N$+122.12
授权中心-手机，$\|p\|$=20	$2.81N$+76.5
授权中心-手机，$\|p\|$=42.5	$2.81N$+163.35
授权中心-手机，$\|p\|$=64	$2.81N$+246.34
*基于证书方案，$\|p\|$=64	$146.99N$
*Merkle 哈希树方案，$\|p\|$=64	$144.56N$
*基于身份方案，$\|p\|$=64	$111.02N$

在传输次数逐渐变多的情况下，本方案的通信能量损耗存在明显的优势。

4.2.3 计算开销　假设传感器的处理器是一个低功耗、高性能、32 bit 英特尔 PXA255 处理器。PXA255 工作在主动和空闲模式的典型功耗分别是 411 mw 和 121 mw，根据文献[26], 32 bit 微处理器上计算 Tate 对大约需要 752 ms，因此在 PXA255 上运行 Tate 配对大约需要 33/400×752≈62.04 ms，使用相同的估算方法，文献[27]中的分析可知校验 1 次 ECDSA-160 签名算法需要耗时 18.48 ms，由于哈希算法和对称加密算法有着极低的计算开销，此处忽略了哈希算法和对称加密算法的开销。

假设每个数据用户进行 N 次数据交互，根据文献[27]基于证书的算法中，计算开销主要由两次 ECDSA 签名认证产生，总开销为 $2\times18.48N=36.96N$ s；在二叉哈希树算法中，计算开销主要是 1 次 ECDSA 签名认证，因此开销为 $18.48N$ ms；基于 ID 的算法中，计算开销主要为两次 Tate 配对，总计算开销为 $2\times62.04N=124.08N$ ms。本文提出的算法中，对于数据用户和数据接收器之间的通信，用户身份认证的计算开销主要为 12 次 Tate 对，总开销为 $12\times62.04=744.48$ ms，认证完成后，在通信密钥更新之前，数据用户无需再计算 Tate 对。授权中心与数据接收器之间的通信，计算开销 24 次的 Tate 对，总开销为 $24\times62.04=1488.96$ ms，当用户认证完成后，数据用户无需再进行 Tate 配对。表 3 展示了计算开销对比。

表 3 计算开销

方案	计算量(ms)
基于证书的方案	$36.96N$
*Merkle 哈希树方案	$18.48N$
*基于身份的方案	$124.08N$
数据用户-手机传输方案	$744.48N$
数据用户-传感器传输方案	$1488.96N$

从表 3 可以得出以下结论：在数据传输次数较少时，本方案由于注重安全性认证，因此产生较大的计算开销，在认证完成后，无需再进行重复认证，因此随着数据传输次数的增加(N>12)，在相同传输次数条件下，本文方案计算开销低的优势逐步体现。其次，随着微型计算机技术的高速发展，处理器性能的不断提升，计算开销将会进一步的降低。

4.3 实验仿真

本节通过仿真实验验证算法整体的计算开销。实验采用斯坦福大学开发的基于 JAVA 的双线性对密码库(JPBC)，椭圆曲线采用 Type A:$y^2=x^3+x$。实验环境为 Inter(R) Core(TM) i5-3230M 2.60 GHz CPU, 12.00 GB 内存，Windows 7 64 bit 操作系统。实验中对称加密采用 128 bit AES 加密算法，不计实际应用中的数据传输延时。

实验对算法最关键的初始化、加密、私钥生成、解密这 4 个步骤进行仿真，结果如图 5–图 8 所示。算法在属性个数不断增加的情况下，消耗时间也随之增加。这是因为随着属性个数增多，算法需生成的属性值、密文组件及需解密的组件均随之增多。

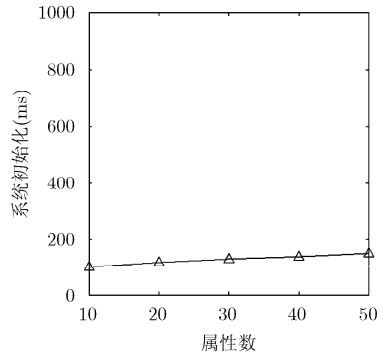

图 5 系统初始化时间

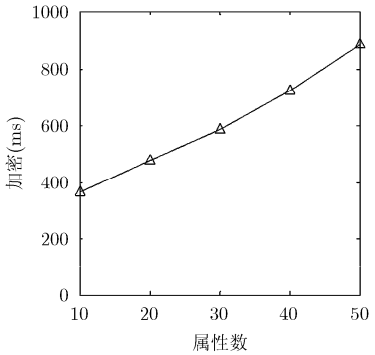

图 6 加密时间

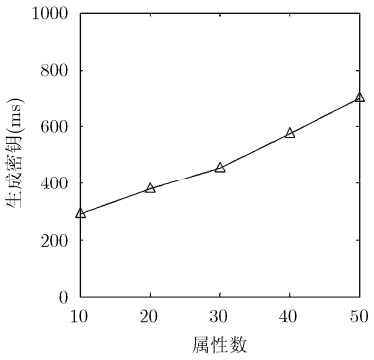

图 7 生成私钥时间

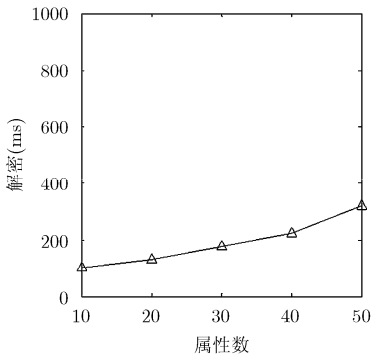

图 8 解密时间

可见，即使当属性个数达到 50，系统仍能够保持一个较短的运行时间,在实际应用中，数据属主可灵活设定访问策略，实现细粒度的访问控制。

5 结束语

本文通过代理重加密技术，为无线脑电信号检测网络提供了一种高效安全的基于属性的访问控制机制，即解决了 BCI 在医疗应用中用户数据的隐私保护与安全问题。性能分析表明，该方案特别适用于用户属性变化频繁、隐私保护要求高并且能耗与计算开销有限的 BCI 应用环境中。

参 考 文 献

[1] WOLPAW J, BIRBAUMER N, and HEETDERKS W. Brain-computer interface technology: A review of the first international meeting[J]. *IEEE Transactions on Rehabilitation Engineering*, 2000, 8(2): 164–173. doi: 10.1109/TRE.2000.847807.

[2] WOLPAW J, BIRBAUMER N, MCFARLAND D J, *et al*. Brain-computer interfaces for communication and control[J]. *Clinical Neurophysiology Official Journal of the International Federation of Clinical Neurophysiology*, 2002, 113(6): 767–791. doi: 10.1016/S1388-2457(02)00057-3.

[3] Abdulkader S N, ATIA A, and MOSTAFA M S M. Brain computer interfacing: Applications and challenges[J]. *Egyptian Informatics Journal*, 2015, 16(2): 213–230. doi: 10.1016/j.eij.2015.06.002.

[4] BLONDET M V R, BADARINATH A, KHANNA C, *et al*. A wearable real-time BCI system based on mobile cloud computing[C]. International IEEE/EMBS Conference on Neural Engineering, San Diego, CA, USA, 2013: 739–742. doi: 10.1109/NER.2013.6696040.

[5] ELSAWY A S and ELDAWLATLY S. P300-based applications for interacting with smart mobile devices[C]. International IEEE/EMBS Conference on Neural Engineering. IEEE, Montpellier, France, 2015: 166–169. doi: 10.1109/NER.2015.7146586.

[6] HONDA K and KUDOH S N. Air brain: The easy telemetric system with smartphone for EEG signal and human behavior[C]. International Conference on Body Area Networks, Brussels, Belgium, 2013: 343–346. doi: 10.4108/icst.bodynets.2013. 253918.

[7] LI Q Q, DING D, and CONTI M. Brain-computer interface applications: Security and privacy challenges[C]. IEEE Communications and Network Security, Florence, Italy, 2015: 663–666. doi: 10.1109/CNS.2015.7346884.

[8] MARTINOVIC I, DAVIES D, FRANK M, *et al*. On the feasibility of side-channel attacks with brain-computer interfaces[C]. Usenix Conference on Security Symposium, Berkeley, CA, USA, 2012: 34.

[9] CHIU Yutzu. Mind reading to predict the success of online games[OL]. http://spectrum.ieee.org/consumer-electronics/gaming/mind-reading-to-predict-the-success-of-online-games .IEEESpectrum, Feb.5, 2013.

[10] LUBER B, FISHER C, APPELBAUM P S, *et al*. Non-invasive brain stimulation in the detection of deception: scientific challenges and ethical consequences[J]. *Behavioral Sciences & the Law*, 2009, 27(2): 191–208. doi: 10.1002/bsl.860.

[11] U.S. Centers for Medicare & Medicaid Services. Hippa basics for providers: privacy, security, and breach notification rules[OL]. https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf. 2016.

[12] U.S. Federal Trade Commission. Federal trade commission act[OL]. https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act.Apr.12, 2015.

[13] CHIZECK H J and BONACI T. Brain-computer interface anonymizer[OL]. https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20140228701.pdf. Aug.14, 2014.

[14] BONACI T, CALO R, and CHIZECK H. App stores for the brain: privacy and security in brain-computer interfaces[J]. *Technology & Society Magazine IEEE*, 2015, 34(2): 32–39.

doi: 10.1109/MTS.2015.2425551.

[15] VENKATASUBRAMANIAN K K, BANERIEE A, and GUPTA S K S. EKG-based key agreement in body sensor networks[C]. INFOCOM Workshops. IEEE, Phoenix, AZ, USA, 2008: 1–6. doi: 10.1109/INFOCOM.2008.4544608.

[16] CHERUKURI S, VENKATASUBRAMANIAN K K, and GUPTA S K S. BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body[C]. International Conference on Parallel Processing Workshops, Kaohsiung, 2003: 432–439. doi: 10.1109/ICPPW.2003.1240399.

[17] TAN C C, WANG H, ZHONG S, *et al*. Body sensor network security: An identity-based cryptography approach[C]. ACM Conference on Wireless Network Security, Alexandria, VA, USA, 2008: 148–153. doi: 10.1145/1352533.1352557.

[18] MALEK B and MIRI A. Combining attribute-based and access systems[C]. 2009 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 2009, 3: 305–312. doi: 10.1109/CSE.2009.157.

[19] HAN R F, WANG H X, XIAO Q, *et al*. A united access control model for systems in collaborative commerce[J]. *Journal of Networks*, 2009, 4(4): 279–289. doi: 10.4304/jnw.4.4.279-289.

[20] WAN Z, LIU J, and DENG R H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. *IEEE Transactions on Information Forensics & Security*, 2012, 7(2): 743–754. doi: 10.1109/TIFS.2011.2172209.

[21] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data [C]. ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, 2006: 89–98. doi: 10.1145/1180405.1180418.

[22] 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1–12. doi: 10.13868/j.cnki.jcr.000001.

FENG Dengguo and CHEN Cheng. Research on attribute-based cryptography[J]. *Journal of Cryptologic Research*, 2014, 1(1): 1–12. doi: 10.13868/j.cnki.jcr.000001.

[23] YU S, WANG C, REN K, *et al*. Attribute based data sharing with attribute revocation[C]. ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010, Beijing, China, 2010: 261–270. doi: 10.1145/1755688.1755720.

[24] NARUSE T, MOHRI M, and SHIRAISHI Y. Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating[J]. *Human-centric Computing and Information Sciences*, 2015, 5(1): 1–13. doi: 10.1186/s13673-015-0027-0.

[25] WANDER A S, GURA N, EBERLE H, *et al*. Energy analysis of public-key cryptography for wireless sensor networks[C]. Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, Kauai Island, HI, USA, 2005: 324–331. doi: 10.1109/PERCOM.2005.18.

[26] BERTONI G M, CHEN L, FRAGNETO P, *et al*. Computing tate pairing on smartcards[OL]. http://citeseerx.ist.psu.edu/viewdoc/download? doi: 10.1.1.83.9125&rep=rep1&type=pdf.

[27] REN Kui, ZENG Kai, LOU Wenjing, *et al*. On broadcast authentication in wireless sensor networks[C]. International Conference on Wireless Algorithms, Systems, and Applications, Xi'an, China, 2006: 502–514. doi: 10.1007/11814856_48.

屠袁飞：男，1984 年生，博士生，助理工程师，研究方向为云计算安全与访问控制.

杨　庚：男，1961 年生，博士，教授，博士生导师，CCF 高级会员、主要研究方向为网络安全、分布与并行计算、大规模科学工程计算等.

袁冯杰：男，1992 年生，硕士生，研究方向为云计算安全与访问控制.