# 面向脑机接口技术的属性可撤销访问控制方案

王 静 司书建

(南京工业大学计算机科学与技术学院 南京 211816)

**摘 要** 脑机接口技术(Brain-Computer Interface,BCI)在康复医学领域被广泛应用,然而其中的隐私数据保护问题常被忽略,从而引发严重的安全威胁,产生隐私泄露的隐患。针对BCI应用中的隐私保护问题,提出一种安全、高效的属性基访问控制方案。该方案利用版本号标记和代理重加密技术实现属性撤销,从而使访问策略灵活多变。实验分析表明,该方案有效地解决了BCI系统中的隐私保护问题,并提高了计算效率,降低了运算复杂度。

**关键词** 脑机接口技术,属性撤销,属性基访问控制,代理重加密,隐私保护

**中图法分类号** TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.09.031

## Attribute Revocable Access Control Scheme for Brain-Computer Interface Technology

WANG Jing SI Shu-jian

(School of Computer Science and Technology,Nanjing Tech University,Nanjing 211816,China)

**Abstract** Though brain-computer interface(BCI) technology has wide application in the field of rehabilitation medicine, the general neglect of private sensitive data protection usually leads to serious security issues. In this paper,a secure and efficient attribute-based access control scheme was proposed for the privacy protection in BCI applications. The new scheme uses the version number tag and proxy re-encryption technology to realize the attribute revocation,which makes the access strategy more flexible. The experimental results show the scheme's capability enhancing the computational efficiency and reducing the computational complexity,as well as its effectiveness in the privacy protection of the BCI system.

**Keywords** Brain-computer interface technology,Attribute revocation,Attribute based access control,Proxy re-encryption,Privacy preservation

## 1 引言

脑机接口技术(Brain-Computer Interface,BCI)形成于20世纪70年代,是一种涉及神经学科、信号检测、模式识别等多学科的交叉技术。随着临床医学、神经生物学和计算机科学等的发展,脑机接口技术被广泛应用于医疗康复、神经科学和军事等领域。2002年,美国国防部在美国的6个实验室中开展"意念控制机器"的研究工作,巨大的经费投入也进一步推动了BCI的全球研究热潮[1-3]。

BCI通过脑电(Electroencephalogram,EEG)传感器采集脑电信号,并通过智能手机将这些信号发送到分析平台进行存储、分析和共享。该系统包含了大量的隐私数据,这些数据的泄露会造成重大损失,甚至危及个人的生命安全。目前,BCI生产商更多地关注面向移动互联网的具体应用程序的开发,忽略了第三方绕过权限读取用户敏感信息[4]的问题,再加上无线网络易被入侵,手机作为数据接收器面临着被偷盗或遗失的风险等,导致数据安全与隐私保护问题突出。

针对上述情况,研究人员提出通过跨学科合作,研究开发防止数据泄露的工具,实现隐私数据的保护,其中加密是目前应用得比较广泛的手段[5]。Tan等[6]提出了一种基于身份的加密(Identity-Based Encryption,IBE)方案,该方案以用户的唯一身份标志作为公钥进行数据加密,保护了传感器数据的隐私,同时能够在轻量级设备上运行,但是该方案没有提出具体的访问控制模型。Gupta等[7-8]提出了一种直接利用传感器对体感信号进行加密的方案,该方案将生理属性(如血压、心率等)作为密钥,拥有相同密钥的用户能够解密数据,但是攻击者如果获得了病人的生理信号,便可直接解密该密文,从而造成隐私数据的泄露。Chizeck等[9-10]针对BCI的安全与隐私保护问题提出了一种匿名方案,该方案提出在存储和传输神经信号之前对信号进行处理,为防止原始神经信号的泄露,除去特定BCI命令外的所有用户信息,仅保留必要的神经信息,然而这也会造成后续分析中因没有足够的数据而不能对用户产生的数据与其包含的信息进行深入挖掘的问题。

为了满足开放网络下隐私数据保护所面临的安全、细粒度控制策略[11-12]等需求,Malek等[13]提出了一种基于属性的访问控制(Attribute-based Access Control,ABAC)。而ABAC

到稿日期:2017-08-23 返修日期:2017-12-09

王 静(1982-),女,博士,副研究员,主要研究方向为无线传感器网络、网络安全;司书建(1992-),男,硕士,主要研究方向为信息安全,E-mail:15950456435@163.com(通信作者)。

的研究有两个方面：基于密钥策略（KP-ABE）和基于密文策略（CP-ABE）的访问控制[14]。其中，CP-ABE 的密文中嵌入了访问控制结构，而密钥则是与用户属性相关。第一个 CP-ABE 算法[15]由 Bethencourt 等人于 2007 年在 S&P 会议上提出。

在实际应用中，用户属性并非固定不变，当这些属性发生变化时，相应的访问策略也应该随之变化，因此属性撤销成为了属性加密（Attribute-Based Encryption，ABE）[15,22-23]必须解决的问题。目前，已有的方案更多地关注如何支持表述能力更为强大的解密策略，并没有充分考虑属性撤销问题，造成在实际应用中系统需要周期性地对数据进行重新加密以及分发新的密钥，增加了系统的负荷。

本文的主要工作是针对 BCI 系统提出一种高效、安全并支持属性可撤销的访问控制方案，本方案支持任意的线性秘密共享方案（Linear Secret Sharing Scheme，LSSS）访问结构，有效地控制了用户权限，保护了数据隐私。算法对以往的密文定长 CP-ABE 算法进行改进，利用版本号标记和代理重加密技术，实现属性的撤销，使得访问策略更加高效、灵活；利用智能手机存储密文，减小了传感器的运算量。

## 2 相关工作及预备知识

### 2.1 双线性映射

设 $G_1$ 和 $G_2$ 是两个 $p$ 阶循环群，其中 $p$ 为大素数。设 $P$ 为 $G_1$ 的生成元，定义双线性映射[16-17] $e:G_1\times G_1\rightarrow G_2$ 满足以下条件。

（1）双线性：对于任意的 $P,Q\in G_1$，$a,b\in Z_p$，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：对于任意的 $P,Q\in G_1$，$a,b\in Z_p$，存在一个有效的多项式时间算法可计算出 $e(P,Q)$。

### 2.2 线性秘密共享体制（LSSS）

一个基于成员集 $P$ 的秘密共享方案[18-19] $\Pi$ 在 $Z_p$ 上是线性的，需要满足以下两个条件。

（1）成员集 $P$ 中的每个成员所分得的秘密信息的一部分构成一个 $Z_p$ 上的矩阵。

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

### 2.3 线性重构

$\Pi$ 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，$I=\{i:x_i|\in S\}\in\{1,2,\cdots,l\}$，那么可以在多项式时间内找出一个常数集$\{\omega_i\in Z_p\}_{i\in I}$，使得$\sum_{i\in I}\omega_i\cdot(M\cdot v)_i=s$。

### 2.4 复杂性假设

判定性双线性 Diffie-Hellman（Decisional Bilinear Diffie-Hellman，DBDH）假设：定义 $a,b,c,z\in_R Z_p$，$g\in_R G$。如果不能在多项式时间内将元组$\lfloor g,g^a,g^b,g^c,g^z\rfloor$与元组$\lfloor g,g^a,g^b,g^c,(g,g)^{abc}\rfloor$以明显的优势区分开，则认为 DBDH 假设成立。

## 3 系统方案

### 3.1 系统模型

一个实时的 BCI 通信系统模型如图 1 所示，其中包含 4 个部分：授权中心（Key Generation Center，KGC）、EEG 传感器（EEG Sensor，ES）、数据接收器（Data Sink，智能手机）以及数据用户（Data Consumers，医生或护士）。

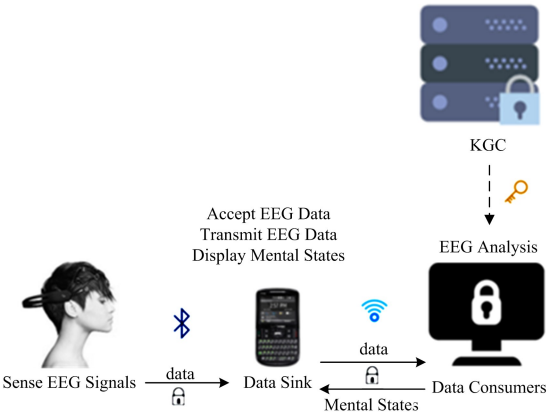


图 1 实时 BCI 通信系统模型

Fig. 1 Real-time BCI communication system model

#### 3.1.1 授权中心

KGC 运行系统初始化程序，生成公钥和主密钥，管理系统的属性。KGC 中保存着主密钥，而公钥保存在传感器中。当发生属性撤销时，KGC 执行重加密算法，生成新的参数，并与手机建立安全、可靠的通信连接，将新参数发送给手机，手机完成对密文的更新。

#### 3.1.2 EEG 传感器

传感器采集病人的脑电信号，利用基于属性的加密方法，根据访问策略对数据进行加密，再将密文发送到手机上。

#### 3.1.3 数据接收器（即智能手机）

智能手机存储已被加密过的病人脑电信号。数据用户从手机中获取该密文，利用自己的属性私钥来解密密文，只有当其属性满足访问策略时才能获得正确的明文数据。

在传统的访问模式中，数据接收器相当于一个代理服务器，完成用户身份认证、权限检查、数据加密及发送功能，扮演着非常重要的角色，需要拥有最高的信任级别，且运算量很大。智能手机作为数据接收器，一旦被偷或丢失，攻击者就能直接获得其中的数据。此外，手机中安装的一些应用程序也可能绕开权限窃取数据，使得手机面临多种风险。

在本模型中，我们假设手机是诚实但好奇的，且易受到攻击。因此，EEG 传感器对数据进行加密后再发送到手机，手机对密文进行存储、更新、转发，其自身也没有访问原始数据的权限，攻击者即使获得该手机，也只能获得密文数据。此外，访问控制策略包含在密文中，用户只有具备相应的属性才能获得访问数据的权限，手机不需做实时、在线的访问控制，从而减少了手机的运算消耗。

#### 3.1.4 数据用户

数据用户一般包括医生、护士。数据用户向 KGC 声明其拥有的属性，以获得属性私钥。当数据用户的属性满足密文

中所设定的访问策略时,数据用户可以通过该私钥对原始数据进行访问。

### 3.2　访问控制模型

本文在文献[20]的加密算法的基础上,提出了一种 BCI 下保护用户隐私的访问控制模型。如图 2 所示,对于某病人的 EEG 数据,访问策略规定只有神经科的主治医师或护士才可以看到其中的具体内容,其逻辑表达式为:({神经科}AND {主治医师 OR 护士})。由于 EEG 数据已按上述访问策略进行加密,因此其他科室人员就无法对该密文进行解密,从而实现了灵活、细粒度的访问控制。

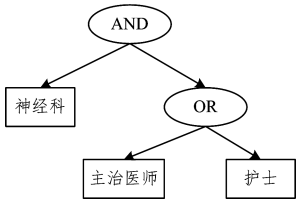


图 2　访问策略

Fig. 2　Access strategy

### 3.3　算法设计

本文算法利用版本号标记和代理重加密技术,实现了属性的撤销。图 3 为加密流程图,加密流程包括了初始化过程。

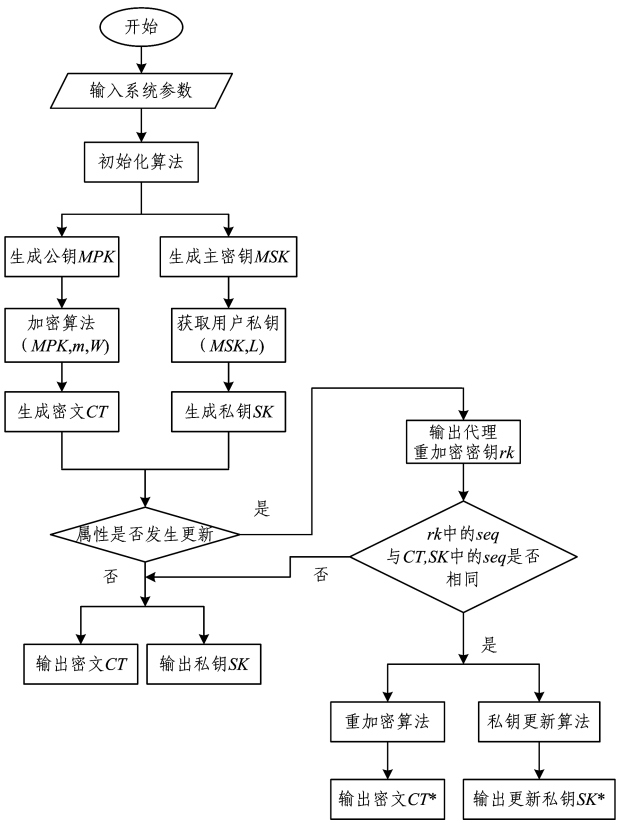


图 3　加密流程图

Fig. 3　Encryption flowchart

加密流程:首先,系统运行初始化算法,生成公钥和主密钥,再以公钥和主密钥作为输入分别运行加密算法和私钥生成算法得到密文 $CT$ 和私钥 $SK$;在输出密文和私钥前,对属性是否发生更新进行判断,如果发生更新,则运行代理重加密算法,并判断是否需要进行密文和私钥更新,若需要则运行重加密算法和私钥更新算法,否则直接输出密文 $CT$ 和私钥 $SK$。

解密流程:当用户的属性集满足属主定义的访问策略时,用户开始解密,得到明文,否则不执行解密。

如图 3 所示,加密算法执行完毕后,生成密文 $CT$ 和私钥 $SK$。用户获得 $CT$,在解密前需要判断是否可以执行解密,解密流程如图 4 所示。

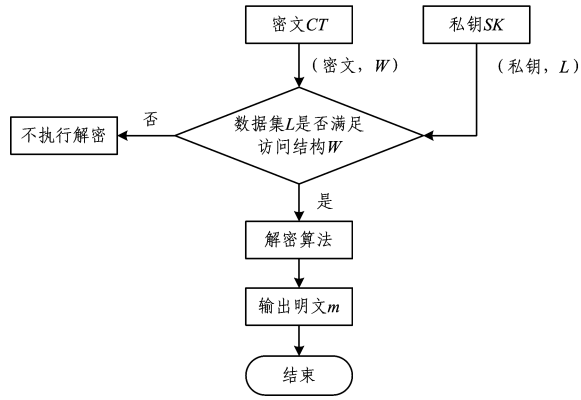


图 4　解密流程图

Fig. 4　Decryption flowchart

步骤 1　系统初始化 Setup($U$)

Step1　KGC 选取一个大素数 $p$,设 $G_1$,$G_2$ 是两个阶为 $p$ 的乘法循环群,定义 $e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射。假定全集中有 $n$ 个属性,用 $U=\{U_1,U_2,\cdots,U_n\}$ 表示,$S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$ 表示 $U_i$ 所有的取值情况,其中 $n_i=|S_i|$。

Step2　KGC 选取 $y\in_R Z_P$,$g,g_1\in_R G_1$,定义 $t_{i,j}\in_R Z_p$ ($i\in[1,n]$),并计算出:

$$Y=e(g,g_1)^y \tag{1}$$

$$T_{i,j}=g^{t_{i,j}} \tag{2}$$

其中,$i\in[1,n]$,$j\in[1,n_i]$。

Step3　初始化版本号 $seq=1$,输出系统公钥为:

$$MPK=\{seq,g,g_1,Y,T_{i,j}\} \tag{3}$$

其中,$i\in[1,n]$,$j\in[1,n_i]$。

主密钥为:

$$MSK=\{seq,y,t_{i,j}\} \tag{4}$$

其中,$i\in[1,n]$,$j\in[1,n_i]$;$seq$ 是初始版本号,标记当前版本,为后文的私钥更新做准备。

$MSK$ 既是系统初始化阶段的输出,又是私钥生成和代理重加密密钥生成的输入,通过其中的 $seq$ 初始化版本号,标记私钥的当前版本。

步骤 2　私钥生成算法 KeyGen($MSK$,$L$)

Step1　输入主密钥 $MSK$ 和一个用户属性列表 $L$,KGC 向该用户发放与属性相关的私钥。KGC 选取 $r\in_R Z_p$,并调用一个 Hash 函数 $H:\{0,1\}^*\rightarrow G$,做如下计算:

$$d_1=g^r \tag{5}$$

$$d_2=g_1^{y+r} \tag{6}$$

$$d_{3,i,j}=(g^{t_{i,j}})^r \tag{7}$$

其中,$v_{i,j}\in L$。

$$d_{4,i,j}=H(v_{i,j})^r \tag{8}$$

其中,$v_{i,j}\in L$。

Step2 生成私钥 $SK$ 为($seq$ 是当前版本号):

$$SK=\{seq,d_1,d_2,d_{3,i,j},d_{4,i,j}\} \tag{9}$$

其中,$v_{i,j}\in L$。

步骤 3 加密算法 Encrypt($MPK,m,W$)

Step1 数据属主定义访问策略 $W$,$W$ 表示$(M,\rho)$,$M$ 表示一个 $l\times n$ 的矩阵,$M_i$ 表示矩阵中的任意行,$i$ 表示行标。函数 $\rho$ 将 $M$ 中的每一行映射到一个用户属性。选取 $s$ ($s\in_R Z_p$),输入系统公钥 $MPK$、LSSS 矩阵访问结构 $W$ 以及信息 $m$,计算出:

$$C_1=mY^s \tag{10}$$

$$C_2=g^s \tag{11}$$

$$C_3=g_1^s \tag{12}$$

$$C_{i,j}=g^{s\cdot t_{i,j}} \tag{13}$$

$$C_4=(\prod_{v_{i,j}\in W}H(v_{i,j}))^s \tag{14}$$

其中,$v_{i,j}\in W$。

Step2 输出密文 $CT$ 如下($seq$ 为当前版本号):

$$CT=\{seq,C_1,C_2,C_3,C_{I,J},C_4\} \tag{15}$$

其中,$v_{i,j}\in W$。

步骤 4 密钥更新算法 KeyUpdate($L^*$,$MSK$)

当属性发生更新时,输入新的属性集合 $L^*\in U$ 和 $MSK$,输出代理重加密的密钥 $rk$。

Step1 $\forall v_{i,j}\in L^*$,选择 $t_{i,j}^*\in Z_p$,计算 $rk_{i,j}=t_{i,j}^*/t_{i,j}$,否则 $rk_{i,j}=1$。

Step2 输出代理重加密的密钥 $rk=\{seq,rk_{i,j}(v_{i,j}\in U)\}$,$seq$ 为当前的版本号,系统的 $seq$ 加 1。

重新选取密钥密文,如果发生用户属性撤销事件,则需要对密文进行一次重加密。

Step1 随机选取一个对称加密密钥 $DEK'$,采用相应的加密算法加密数据文件。

Step2 调用本文的 Encrypt 算法加密 $DEK'$,输出 $CT'$。

步骤 5 重加密算法 ReEncrypt($CT,rk,W$)

Step1 验证 $CT$ 中的 $seq$ 与 $rk$ 中的 $seq$ 是否相同,如果两者不同,则输出密文 $CT$。

Step2 若相同,对于 $\forall v_{i,j}\in W$,计算 $C_{i,j}^*=C_{i,j}^{rk_{i,j}}$,$C_4^*=C_4^{\prod_{v_{i,j}\in W}rk_{i,j}}$。

Step3 输出密文 $CT^*=\{seq+1,C_1,C_2,C_3,C_{I,J}(v_{i,j}\in W),C_4^*\}$,$seq$ 为 $CT$ 中的版本号。

步骤 6 私钥更新算法 ReKeyGen($SK,rk,L$)

Step1 验证用户 $SK$ 中的 $seq$ 与 $rk$ 中的 $seq$ 是否相同,如果两者不同,则输出 $SK$。

Step2 若相同,对于 $\forall v_{i,j}\in L$,计算 $d_{3,i,j}^*=d_{3,i,j}^{rk_{i,j}}$,$d_{4,i,j}^*=d_{4,i,j}^{rk_3}$。

Step3 输出用户私钥为:

$$SK^*=\{seq+1,d_1,d_2,d_{3,i,j}^*,d_{4,i,j}^*\}。$$

其中,$v_{i,j}\in L$。

步骤 7 解密算法 Decrypt($SK,CT$)

Step1 用户获得 $CT$,首先通过下面的等式检验用户属性是否满足文件访问策略。

$$e(d_1,C_4)=e(\prod_{v_{i,j}\in L}d_{4,i,j},C_2) \tag{16}$$

当用户的属性集满足数据属主定义的访问策略时,等式成立,用户开始解密;否则直接返回⊥。

Step2 验证通过后进行如下运算,解密得到明文 $m$(即 $DEK$)为:

$$m=\frac{C_1\cdot e(d_1,C_3\prod_{v_{i,j}\in W}C_{i,j})}{e(C_2,d_2\prod_{v_{i,j}\in L}d_{3,i,j})} \tag{17}$$

下面验证公式的正确性。

首先对验证访问策略的过程进行证明,当用户的属性集满足数据属主定义的访问策略时,以下等式成立:

$$\begin{aligned}e(d_1,C_4)&=e(g^r,(\prod_{v_{i,j}\in W}H(v_{i,j}))^s)\\&=e(g^s,\prod_{v_{i,j}\in L}(H(v_{i,j})^r))\\&=e(\prod_{v_{i,j}\in L}d_{4,i,j},C_2)\end{aligned} \tag{18}$$

可知,上述等式成立时,用户属性集满足访问策略。通过验证访问策略的步骤之后,用户可以进行如下解密过程:

$$\begin{aligned}m&=\frac{C_1\cdot e(d_1,C_3\prod_{v_{i,j}\in W}C_{i,j})}{e(C_2,d_2\prod_{v_{i,j}\in L}d_{3,i,j})}\\&=\frac{mY^s\cdot e(g^r,g_1^s\cdot(\prod_{v_{i,j}\in W}g^{t_{i,j}})^s)}{e(g^s,g_1^{y+r}\cdot\prod_{v_{i,j}\in L}(g^{t_{i,j}})^r)}\\&=\frac{me(g,g_1)^{ys}\cdot e(g,g_1)^{rs}\cdot e(g,g)^{rs\sum_{v_{i,j}\in W}t_{i,j}}}{e(g,g_1)^{(y+r)s}\cdot e(g,g)^{sr\sum_{v_{i,j}\in L}t_{i,j}}}\\&=m\end{aligned} \tag{19}$$

当属性撤销事件发生时,部分密文与密钥的组件将会发生变动。

$rk_{i,j}=t_{i,j}^*/t_{i,j}$,$d_{3,i,j}^*=d_{3,i,j}^{rk_{i,j}}=g^{r\cdot t_{i,j}\cdot rk_{i,j}}$,$d_{4,i,j}^*=d_{4,i,j}^{rk_{i,j}}=H(v_{i,j})^{r\cdot rk_{i,j}}$,$C_{i,j}^*=C_{i,j}^{rk_{i,j}}=g^{s\cdot t_{i,j}\cdot rk_{i,j}}$,$C_4^*=C_4^{\prod_{v_{i,j}\in W}rk_{i,j}}=(\prod_{v_{i,j}\in W}H(v_{i,j}))_4^{s\cdot\prod_{v_{i,j}\in W}rk_{i,j}}$,匹配和解密分别如下:

$$\begin{aligned}e(d_1,C_4^*)&=e(g^r,(\prod_{v_{i,j}\in W}H(v_{i,j}))^{s\cdot\prod_{v_{i,j}\in W}rk_{i,j}})\\&=e(g^s,\prod_{v_{i,j}\in L}(H(v_{i,j})^{r\cdot rk_{i,j}}))\\&=e(\prod_{v_{i,j}\in L}d_{4,i,j}^*,C_2)\end{aligned} \tag{20}$$

$$\begin{aligned}m&=\frac{C_1\cdot e(d_1,C_3\prod_{v_{i,j}\in W}C_{i,j}^*)}{e(C_2,d_2\prod_{v_{i,j}\in L}d_{3,i,j}^*)}\\&=\frac{mY^s\cdot e(g^r,g_1^s\cdot(\prod_{v_{i,j}\in W}g^{t_{i,j}\cdot rk_{i,j}})^s)}{e(g^s,g_1^{y+r}\cdot\prod_{v_{i,j}\in L}(g^{t_{i,j}\cdot rk_{i,j}})^r)}\\&=\frac{me(g,g_1)^{ys}\cdot e(g,g_1)^{rs}\cdot e(g,g)^{rs\sum_{v_{i,j}\in W}t_{i,j}\cdot rk_{i,j}}}{e(g,g_1)^{(y+r)s}\cdot e(g,g)^{sr\sum_{v_{i,j}\in L}t_{i,j}\cdot rk_{i,j}}}\\&=m\end{aligned} \tag{21}$$

式(17)的正确性得证。

### 3.4 数据用户访问数据的过程

由于 ABE 算法本身的复杂性,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。EEG 传感器首先随机选取会话密钥 $K$ 作为 AES 算法的输入,通过该算法加密 EEG 数据,再通过本文提出的 Encrypt 算法加密上述密钥 $K$,得到密钥密文 $CT$。

以下过程解释了一个拥有属性集 $S$ 的用户获取密文的步骤:

Step 1　EEG 传感器从密钥空间中随机地选取一个会话密钥 $K$,利用 AES 算法 AES($K$,$D$)加密 EEG 信号 $D$。

Step 2　定义该文件的访问结构。

Step 3　EEG 传感器调用本文中的 Encrypt 算法加密上述会话密钥 $K$,得到密钥密文 $CT$,再将文件发送至手机。其中 EEG→DS 表示由传感器至手机的数据传输。

$$(\text{Encrypt}(K),\text{AES}(K,D))_{\text{EEG}\to\text{DS}} \tag{22}$$

Step 4　用户向 KGC 声明其所拥有的属性,调用 KeyGen 算法获得属性私钥。

Step 5　用户从智能手机中获取加密数据,再调用 Decrypt 算法得到会话密钥 $K$。

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

### 3.5　数据用户属性撤销时的安全通信

在发生属性撤销的情况下,KGC 需要执行密钥更新算法,以保存主密钥 $MSK'$和重加密密钥 $rk$,并将公钥 $MPK'$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、安全的身份证明方案,以确保 KGC 与手机及传感器间通信的安全。

在这一过程中,EEG 传感器根据访问策略对访问令牌 $K_1$ 进行加密,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 进行第二次挑战,如果第二次挑战通过,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、通讯建立阶段以及通讯阶段,下面将详细描述 3 个阶段的过程。

#### 3.5.1　初始化阶段

Step 1　KGC 调用 Setup 算法生成 $MPK$,并且为属性拥有者如医生、护士分配相应的属性。

Step 2　KGC 为相应的医生和护士分别配备其属性私钥,医生为 $SK_D$,护士为 $SK_N$。

Step 3　在为病人佩戴 EEG 传感器之前,先存储公钥 $MPK$。

#### 3.5.2　通讯建立阶段

Step 1　传感器随机选取一个访问标记 $K_1$,调用 Encrypt 加密 $K_{\text{Tdate}}=K_1 \parallel datetime$,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。

$$(\text{Encrypt}(K_{\text{Tdate}}),\text{Hash}(K_{\text{Tdate}}))\mid_{\text{EEG}\to\text{DS}} \tag{23}$$

其中,Hash()表示发送端与接收端协议预先约定的哈希函数。

Step 2　传感器定时地更新访问标记 $K_{\text{Tdate}}$。

Step 3　KGC 获取(Encrypt($K_{\text{Tdate}}$))后,调用 Decrypt 解密密文,并做哈希运算,再发回手机,供传感器读取验证。

Step 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 $K_1'$,调用 Encrypt 算法,以相同的访问结构对 $K'_{\text{Tdate}}=K_1' \parallel datetime$ 进行加密,再将其发送到手机并覆盖原有访问标记,KGC 读取新标记进行二次验证。

$$(\text{Encrypt}(K'_{\text{Tdate}}),\text{Hash}(K'_{\text{Tdate}}))\mid_{\text{EEG}\to\text{DS}} \tag{24}$$

Step 5　KGC 解密(Encrypt($K'_{\text{Tdate}}$)),然后将获得的访问标记的哈希值 $H'=H(K_1' \parallel datetime)$发送回手机。

$$H'=H(K_1' \parallel datetime)\mid_{\text{KGC}\to\text{DS}} \tag{25}$$

Step 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。

#### 3.5.3　通讯阶段

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

$$(AES(K_1',MPK' \parallel rk_{y\to y^{(n)}}),\text{Hash}(MPK' \parallel rk_{y\to y^{(n)}}))\mid_{KGC\to DS} \tag{26}$$

Step 2　传感器读取手机,解密消息得到 $MPK'$,$rk_{y\to y^{(n)}}$,然后比较($H'=\text{Hash}(MPK' \parallel rk_{y\to y^{(n)}})$)是否与 $H$ 相等,如果相等,则消息的完整性得以证明。

Step 3　传感器用 $MPK'$更新原有公钥,并将 $rk_{y\to y^{(n)}}$ 发送到手机,由手机更新密文。

## 4　实验与分析

### 4.1　安全性分析

(1)数据安全性方面。本方案中,数据文件的安全性由 AES 的安全性决定,而 AES 的安全性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,即若攻击者的属性集不满足访问策略,就无法解密密文。智能手机也是加密方案的一部分,但是由于其只是将得到的密钥与密文组件相乘,该密钥并没有关联到用户属性,因此智能手机无法破解密文。

(2)抗合谋攻击方面。防止用户合谋进行攻击是基于属性加密需要解决的问题。在密文策略属性加密中,密文 $CT$ 中嵌入了秘密共享值 $s$。用户(包括合谋攻击者)想要解开密文,则需要计算出 $e(g,g_1)^{ys}$ 的值。为了计算出 $e(g,g_1)^{ys}$,合谋攻击者会利用密文组件 $C_i$,$CT^*$ 和其他合谋用户的私钥组件 $L$,$d_i$ 进行双线性配对运算。而用户的私钥是通过随机数 $r$ 唯一生成,因为用户的 $r$ 不同,所以用户的私钥也不同,即使用户进行合谋攻击,$e(g,g_1)^{ys}$ 的值也不会被计算出。因此只有在用户的属性满足访问策略的情况下,才能正确计算出 $e(g,g_1)^{ys}$ 的值。

### 4.2　安全性证明

**定理 1**　文中方案是基于 DBDH 假设安全的。

设 $\sum_{v_i\in L}t_{h_i,i}\neq\sum_{v_i\in L'}t_{h_i,i}$,若存在 $L$ 与 $L'(L\neq L')$,使得 $\sum_{v_i\in L}t_{h_i,i}=\sum_{v_i\in L'}t_{h_i,i}$,则带有属性集 $L'$的用户可以解密带有属性集 $L$ 的密文;又知有不等式:

$$\frac{p(p-1)\cdots(p-(N-1))}{p^N}>\frac{(p-(N-1))^N}{p^N}=$$
$$(1-\frac{N-1}{p})^N>1-\frac{N(N-1)}{p}>1-\frac{N^2}{p} \tag{27}$$

成立,其中 $N=2^n$,$p$ 为 $G_1$ 的阶数。因此,若每个 $t_{h_i,i}$ 都从 $Z_p$

中随机选出，则 $\sum_{v_i\in L} t_{h_i,i} \neq \sum_{v_i\in L'} t_{h_i,i}$ 这个假设将以非常大的优势成立。假设攻击者 $A$ 赢得游戏的优势为 $\varepsilon$，则可以构造一个算法以一定的优势攻破 DBDH 假设。

Setup 挑战者 $C$ 选取 $a,b,c,z\in_R Z_p$，$v\in_R\{0,1\}$ 和 $G_1$ 的生成元 $g$，当 $v=0$ 时，令 $Z=e(g,g)^{abc}$，否则 $Z=e(g,g)^z$。$C$ 将得到 $\{g,g^a,g^b,g^c,z\}$。现在 $A$ 向 $C$ 发送挑战的访问策略 $W^*$，设 $W^*=\lfloor W_1^*,W_2^*,\cdots,W_f^*\rfloor$。$C$ 进行如下运算：

(1)选择一个 Hash 函数 $H:\{0,1\}^*\rightarrow\{0,1\}^f$，随机选择一个 $\tau'\in Z_p^{2\times f}$，其中：

$$\tau'=\begin{pmatrix} t'_{0,1} & \cdots & t'_{0,f} \\ t'_{1,1} & \cdots & t'_{1,f} \end{pmatrix} \tag{28}$$

(2)计算 $h^*=H(w_1^*\parallel\cdots\parallel w_f^*)$，其中 $w_i^*\in W^*$，计算

$$g^{\tau}=\begin{pmatrix} g^{t_{0,1}\cdots t_{0,n}} \\ g^{t_{1,1}\cdots t_{1,n}} \end{pmatrix} \tag{29}$$

当 $i\in[1,n-1]$ 时，$g^{t_{h_i^*,i}}=g^{t'_{h_i^*,i}\cdots}$，$g^{t_{h_i^*,i}}=g^{t'_{h_i^*,i}}$；另外，$g^{t_{h_n^*,n}}=g^{t'_{h_n^*,n}\cdots}$，$g^{t_{h_n^*,n}}=g^{t'_{h_n^*,n}}$。

(3)得到 $MPK=\{g,g_1=g^a,Y=e(g,g)^{ab},g^{\tau},H\}$ 和 $MSK=\{h^*,\tau'\}$。

Phase1 对于一个由 $A$ 任意定义的属性集 $L=\{v_1,\cdots,v_n\}(L\neq W^*)$，$C$ 经如下计算可以得到解密密钥：

(1)对于每一个 $v_i\in L$，计算 $h=H(v_1\parallel\cdots\parallel v_n)$；

(2)若 $h^*\oplus h=0^n$ or $1^n$，则 $C$ 终止计算；

(3)设 $sum=0$，当 $i\in[1,n-1]$ 时，若 $h_i^*=h_i$，则 $sum=sum+1$；若 $h_n^*=h_n$，则 $sum=sum+n$；

(4)对属性集 $L$ 设置解密密钥：

$$d_1=g^{r-sum^{-1}\cdot a} \tag{30}$$

$$d_2=g^{ab} \tag{31}$$

$$d_3=g^{rx+sum\cdot b-sum^{-1}\cdot x\cdot a-ab}=g^{(r-sum^{-1}\cdot a)(r+sum\cdot b)} \tag{32}$$

其中，$x=\sum_{i\in[1,n]} t'_{h_i,i}$，$r\in_R Z_p$。由等式 $\prod_{i\in[1,n]} g^{t_{h_i,i}}=g^{x+sum\cdot b}$ 可知解密密钥正确，即只要知道 $r,x,sum$ 的值，就能正确地生成解密密钥。

Challenge 对于两个等长的密文 $m_0^*$ 和 $m_1^*$，$C$ 随机地选择 $\mu\in\{0,1\}$，并设置 $C^*=\{W^*,C_1^*,C_2^*,C_3^*\}$，其中 $C_1^*=m_{\mu}^*\cdot Z,C_2^*=g^c,C_3^*=\prod_{i\in[1,n]} g^{c\cdot t_{h_i^*,i}}$。

因此，$\prod_{i\in[1,n]} g^{c\cdot t_{h_i^*,i}}=\prod_{i\in[1,n]} g^{c\cdot t'_{h_i,i}}$，且只要 $C$ 得到 $\tau$，就能有效地生成挑战密文。若 $Z=e(g,g)^{abc}$，则可以正确得到 $C^*$，否则 $A$ 将得不到 $m_{\mu}^*$ 的任何相关信息。

Phase2 同 Phase1 一样。

Guess $A$ 输出猜测 $u'\in\{0,1\}$。如果 $u'=u$，则 $C$ 输出 1，否则输出 0。若 $C$ 不中止，$A$ 将得到由本算法加密得出的信息，且 $C$ 对于解决 DBDH 问题还拥有不可忽略的优势。假设 $C$ 不中止，为攻破方案，在 $Z=e(g,g)^{abc}$ 时，$A$ 的优势为 $\varepsilon$，否则为 0。因此不论 $Z$ 为何值，$C$ 攻破 DBDH 假设的优势都为 $\frac{1}{2}\varepsilon$，用 $\bar{\omega}$ 表示 $C$ 不中止，假设 $A$ 进行了 $q$ 次查询，对于每一次查询，$C$ 不中止的概率为 $1-\frac{1}{2^{n-1}}$，因此对于 $q$ 次查询，概率为 $\Pr[\bar{\omega}]=(1-\frac{1}{2^{n-1}})^q\approx 1-\frac{q}{2^{n-1}}$。

综上所述，$C$ 攻破 DBDH 假设的优势为 $\frac{1}{2}(1-\frac{q}{2^{n-1}})\varepsilon$，因此本文所提方案是基于 DBDH 安全的。

### 4.3 效率分析

本方案采用的属性撤销方案沿用了文献[12]的版本号标记法，表 1 将本方案与文献[12]做比较。为了简化对比方式，做如下定义：$|G_1|$ 是 $G_1$ 中元素的长度（$|G_2|$ 类似），$|Z_p|$ 是 $Z_p$ 的长度，$n$ 是所有属性的个数，$n'=\sum_{i-1}^{n} n_i$ 为所有属性的所有取值情况。

表 1 本方案与文献[12]方案的密钥和密文的长度比较

Table 1 Length comparison of encryption keys and ciphertexts between our scheme and scheme in ref.[12]

| 密钥/密文 | 文献[12]方案 | 本文方案 |
|---|---|---|
| 公钥 | $(3n+1)\|G_1\|+\|G_2\|$ | $2\|G_1\|+\|G_2\|+n'\|Z_p\|$ |
| 主密钥 | $(3n+1)\|Z_p\|$ | $(n'+1)\|Z_p\|$ |
| 私钥 | $(2n+1)\|G_1\|$ | $3\|G_1\|$ |
| 密文 | $(n+1)\|G_1\|+\|G_2\|$ | $2\|G_1\|+G_2$ |

由于方案[12]仅支持带有通配符与属性正负值的与门，而本方案采用的是支持属性可以取多值的与门，因此在表达方式上，本方案的可扩展性更好。本文的密钥及密文长度较方案[12]有明显的优势，当用户属性个数 $n$ 增加时，本文的公钥和主密钥也同样存在明显的优势。表 2 从是否隐藏访问策略与是否支持属性撤销两方面将本文与其他已有方案进行比较。

表 2 3 种方案是否隐藏访问策略与支持属性撤销的对比

Table 2 Comparison of three schemes wether hiding access strategy and supporting attribute revocation or not

| 方案 | 隐藏访问策略 | 属性撤销 |
|---|---|---|
| 文献[21]方案 | 是 | 否 |
| 文献[12]方案 | 否 | 是 |
| 本文方案 | 是 | 是 |

通过对比可以发现，本文同时实现了隐藏访问策略与属性撤销，访问策略更加高效、灵活。

### 4.4 实验仿真

本实验的运行环境为：Inter(R)Core(TM)i5-3470 3.20 GHz CPU，4 GB 内存，操作系统为 Windows 7 32 位。采用斯坦福大学提供的 JPBC 库，椭圆曲线采用 Type $A$：$y^2=x^3+x$。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。

实验主要将本文方案与文献[12]方案进行对比，两种方案的加密、私钥生成和解密 3 个步骤的对比数据如表 3－表 5 所列，仿真结果如图 5－图 7 所示。用户属性个数不断增加，算法消耗时间也随之增加，因为随着属性个数的增加，算法生成的属性值、密文组件和解密组件都将增加。

表 3 本文方案与文献[12]方案的加密时间的比较

Table 3 Comparison of encryption time between our scheme and scheme in ref.[12]

| 属性数/个 | 本方案的加密时间/ms | 文献[12]方案的加密时间/ms |
|---|---|---|
| 10 | 360 | 380 |
| 20 | 440 | 480 |
| 30 | 500 | 570 |
| 40 | 560 | 720 |
| 50 | 640 | 860 |

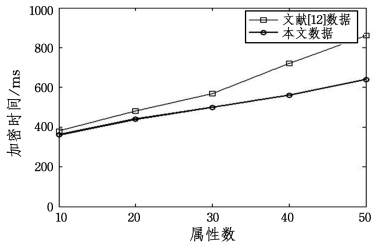


图 5　加密时间的对比结果

Fig. 5　Comparison results of encryption time

表 4　本文方案与文献[12]方案的私钥生成时间的比较

Table 4　Comparison of generation time of private keys between our scheme and scheme in ref. [12]

| 属性数/个 | 本文方案的私钥生成时间/ms | 文献[12]方案的私钥生成时间/ms |
|---|---|---|
| 10 | 250 | 280 |
| 20 | 330 | 380 |
| 30 | 400 | 460 |
| 40 | 490 | 570 |
| 50 | 560 | 700 |

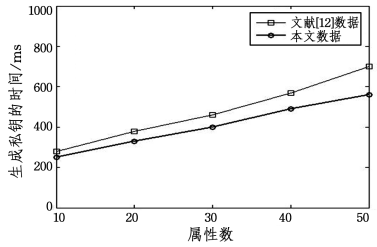


图 6　私钥生成时间的对比结果

Fig. 6　Comparison results of generation time of private keys

表 5　本文方案与文献[12]方案的解密时间的比较

Table 5　Comparison of decryption time between our scheme and scheme in ref. [12]

| 属性数/个 | 本方案的解密时间/ms | 文献[12]方案的解密时间/ms |
|---|---|---|
| 10 | 80 | 100 |
| 20 | 100 | 130 |
| 30 | 120 | 170 |
| 40 | 170 | 220 |
| 50 | 230 | 320 |

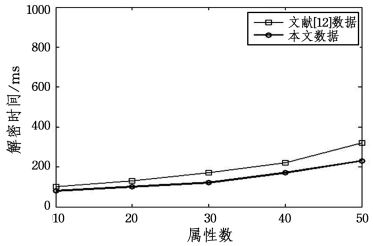


图 7　解密时间的对比结果

Fig. 7　Comparison results of decryption time

由表 3－表 5 和图 5－图 7 可知，与文献[12]方案相比，本文方案的系统加密时间、私钥生成时间和解密时间有了大幅缩减，尤其是随着用户属性个数的增加，时间缩减得越来越明显，效果越来越显著。在实际应用中，数据属主可灵活设置访问策略，实现细粒度的访问控制。

**结束语**　本文通过版本号标记和代理重加密技术，为脑机接口技术提出了一种安全、高效并支持属性可撤销的访问控制。实验分析表明，本方案较好地解决了 BCI 在实际应用中用户数据隐私的保护和安全问题，特别适合用于用户属性变化频繁、隐私保护级别较高的 BCI 系统中。

## 参 考 文 献

[1] WOLPAW J R, MCFARLAND D J, BIRBAUMER N, 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.

[2] WOLPAW J R, HEETDERKS W J, BIRBAUMER N, et al. Brain-computer interface technology: a review of the first international meeting[J]. IEEE Transactions on Rehabilitation Engineering A Publication of the IEEE Engineering in Medicine & Biology Society, 2000, 8(2): 164-173.

[3] ABDULKADER S N, ATIA A, MOSTAFA M S M. Brain computer interfacing: Applications and challenges[J]. Egyptian Informatics Journal, 2015, 16(2): 213-230.

[4] LI Q Q, DING D, CONTI M. Brain-Computer Interface applications: security and privacy challenges[C]// Communications and Network Security. IEEE, 2015.

[5] LEE K Y, JANG D. Ethical and social issues behind brain-computer interface[C]// International Winter Workshop on Brain-Computer Interface. 2013: 72-75.

[6] 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. 2008: 148-153.

[7] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S, et al. EKG-based key agreement in Body Sensor Networks [C]// INFOCOM Workshops. IEEE, 2008: 1-6.

[8] CHERUKURI S, VENKATASUBRAMANIAN K K, GUPTA S K S. Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body[C]// Workshop on International Conference on in Wireless Networks of Biosensors Implanted in the Human Body. 2003: 432-439.

[9] CHIZECK H J, BROWN T, THOMPSON M C, et al. Controlling our brains â a case study on the implications of brain-computer interface-triggered deep brain stimulation for essential tremor[J]. Brain-Computer Interfaces, 2016, 3(4): 165-170.

[10] BONACI T, CALO R, CHIZECK H J. App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces[J]. Technology & Society Magazine IEEE, 2015, 34(2): 32-39.

[11] FENG D G, CHEN C. Research on attribute-based cryptography [J]. Journal of Cryptologic Research, 2014, 1(1): 1-12. (in Chinese)
冯登国，陈成. 属性密码学研究[J]. 密码学报，2014，1(1)：1-12.

[12] 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.

[13] MALEK B, MIRI A. Combining attribute-based and access systems[C]// International Conference on Computational Science and Engineering. 2009:305-312.

[14] 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. 2006:89-98.

[15] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security and Privacy. 2007:321-334.

[16] DAN B, FRAKLIN M. Identity based encryption from the Weil pairing: Advances in Cryptology[J]. Lecture Notes in Computer Science, 2003, 32(3):213-229.

[17] XIA C, ZHOU J S. Research on cloud manufacturing resource-aware and access technology using RFID[J]. Journal of Harbin Institute of Technology, 2014, 21(3):101-110.

[18] LIU Z, CAO Z F. On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption [J/OL]. http://www.iacr.org/cryptodb/data/paper.phb?pubkey=23275.

[19] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Israel: Technion-Israel Institute of Technology, Faculty of Computer Science, 1996.

[20] NARUES T, MOHRI M, 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.

[21] ZHANG Y H, CHEN X F, LI J, et al. Anonymous attribute-based encryption supporting efficient decrypyion test[C]// Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. 2013:511-516.

[22] PHUONG T V X, YANG G, SUSILO W. Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions [J]. IEEE Transactions on Information Forensics & Security, 2015, 11(1):35-45.

[23] JIN C, FENG X, SHEN Q. Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size[C]// International Conference on Communication and Network Security. ACM, 2016:91-98.

(上接第 186 页)

## 参 考 文 献

[1] 吴世忠,郭涛,董国伟,等. 软件漏洞分析技术[M]. 北京:科学出版社,2014.

[2] WU J X. Meaning and Vision of Mimic Computing and Mimic Security Defense[J]. Telecommunications Science, 2014, 30(7):2-7. (in Chinese)
邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7):2-7.

[3] WU J X. Mimic Security Defense in Cyber Space[J]. Secrecy Science and Technology, 2014(10):4-9. (in Chinese)
邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014(10):4-9.

[4] WU J X. Research on Cyber Mimic Defense[J]. Journal of Cyber Security, 2016, 1(4):1-10. (in Chinese)
邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4):1-10.

[5] MARVIN R. System Reliability Theory: Models, Statistical Methods, and Applications (Second Edition)[M]. Beijing: National Defend Industry Press, 2011. (in Chinese)
MARVIN R. 系统可靠性理论:模型、统计方法及应用(第 2 版)[M]. 北京:国防工业出版社, 2011.

[6] SUN H Y, LIU B, CAO X L. Research on reliability and security of vote redundancy system[J]. Journal of Electronic Measurement and Instrument, 2011, 25(7):661-664. (in Chinese)
孙怀义, 刘斌, 曹晓莉. 表决冗余系统可靠性与安全性研究[J]. 电子测量与仪器学报, 2011, 25(7):661-664.

[7] LI C Y, CHEN X, YI X S, et al. Analysis of k—out-of-n:G systems subject to common cause failures based on Markov process [J]. Systems Engineering and Electronics, 2009, 31(11):2789-2792. (in Chinese)
李春洋, 陈循, 易晓山, 等. 基于马尔可夫过程的 k/n(G)系统共因失效分析[J]. 系统工程与电子技术, 2009, 31(11):2789-2792.

[8] LIU Y, LI R Z, ZHANG G B. Reliability analysis of k/n(G) Markov system with non-homogenous units[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015, 43(3):17-21. (in Chinese)
刘英, 李荣祖, 张根保. 非同型单元 k/n(G)马尔可夫系统可靠性分析[J]. 华中科技大学学报(自然科学版), 2015, 43(3):17-21.

[9] YIN L H, FANG B X. Security Attributes Analysis for Intrusion Tolerant Systems[J]. Chinese Journal of Computers, 2006, 29(8):1505-1512. (in Chinese)
殷丽华, 方滨兴. 入侵容忍系统安全属性分析[J]. 计算机学报, 2006, 29(8):1505-1512.

[10] MADAN B B, GOSEVA-POPSTOJANOVA K, VAIDYANATHAN K, et al. A method for modeling and quantifying the security attributes of intrusion tolerant systems [J]. Performance Evaluation, 2004, 56(1-4):167-186.

[11] ZANG H W, HAN W, GAO D Y. Dissimilar redundancy computer system and reliability analysis[J]. Journal of Harbin Institute of Technology, 2008, 40(3):492-494. (in Chinese)
臧红伟, 韩炜, 高德远. 非相似余度计算机系统及其可靠性分析[J]. 哈尔滨工业大学学报, 2008, 40(3):492-494.

[12] YE Y, XU X S, JIA Y, et al. An Attack Graph-Based Probabilistic Computing Approach of Network Security[J]. Chinese Journal of Computers, 2010, 33(10):1987-1996. (in Chinese)
叶云, 徐锡山, 贾焰, 等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报, 2010, 33(10):1987-1996.