一种适用于工业控制系统的加密传输方案

屠袁飞*①② 苏清健① 杨 庚②
①(南京工业大学计算机与科学技术学院 南京 211800)
②(南京邮电大学计算机学院 南京 210003)

摘 要：随着工业物联网(IoT)、云计算等信息技术与工业控制系统(ICS)的整合，工业数据的安全正面临着极大风险。为了能在这样一个复杂的分布式环境中保护数据的机密性和完整性，该文采用基于属性的加密(ABE)算法，设计一种集数据加密、访问控制、解密外包、数据验证为一体的通信方案，同时具有密文长度恒定的特点。最后，从正确性、安全性和性能开销3个方面对方案进行详细的分析，并通过仿真验证得出该算法具有低解密开销的优势。

关键词：工业控制系统；机密性；解密外包；密文定长；数据验证
中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)02-0348-07
DOI: 10.11999/JEIT190187

An Encryption Transmission Scheme for Industrial Control System

TU Yuanfei①② SU Qingjian① YANG Geng②
①(*College of Computer Science and Technology, Nanjing University of Technology, Nanjing* 211800, *China*)
②(*College of Computer Science and Technology, Nanjing University of Post and Telecommunication, Nanjing* 210003, *China*)

Abstract: With the integration of information technology such as industrial Internet of Things (IoT), cloud computing and Industrial Control System (ICS), the security of industrial data is at enormous risk. In order to protect the confidentiality and integrity of data in such a complex distributed environment, a communication scheme is proposed based on Attribute-Based Encryption (ABE) algorithm, which integrates data encryption, access control, decryption outsourcing and data verification. In addition, it has the characteristics of constant ciphertext length. Finally, the scheme is analyzed in detail from three aspectsie correctness, security and performance overhead. The simulation results show that the algorithm has the advantage of low decryption overhead.

Key words: Industrial Control System (ICS); Confidentiality; Decryption outsourcing; Constant ciphertext length; Data verification

1 引言

随着工业控制系统(Industrial Control System, ICS)和信息技术(Information Technology, IT)加速融合，原本独立、封闭的工控系统开始使用云计算、大数据等技术进行数据的存储及分析[1]。在这一过程中，工控系统面临着来自外部网络的多种威胁，如恶意入侵、计算机病毒、网络攻击等，最知名的是2010年伊朗“Stuxnet”病毒事件[2]。在传统的工业控制系统中，数据以明文形式进行传输，如果将明文数据直接发送并存储到云平台，则可能导致数据面临泄露、被篡改等威胁，造成无法挽回的损失[3,4]。近年来，世界各国均提出了一些极具参考意义的指标和安全实践指南，我国也颁布了《网络安全法》，提出加强关键信息基础设施安全防护，维护国家网络安全[5]。

为保障工业数据的机密性，加密无疑是一种有效方案，对此，多位学者进行了研究。Halas等人[6]在PLC(Programmable Logic Controller)中对3DES(Triple Data Encryption Algorithm)和AES(Advanced Encryption Standard)分别进行了仿真测试，结果显示AES算法性能较好，能够满足实时性要求，但是密钥的分发和管理工作还未得到很好的解决。之后，为达到更高的安全性，文献[7,8]

收稿日期：2019-03-27；改回日期：2019-07-20；网络出版：2019-09-27
*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)
Foundation Items: The National Natural Science Foundation of China (61572263, 61272084), The Natural Science Foundation of the Jiangsu Province Higher Education Institutions (11KJA520002)

改进了一种半同态加密算法，并将其应用在PLC上，以实现加密控制器的功能，然而结果显示PLC的计算开销较大，不能满足控制系统所必需的实时性要求。可见，由于工控系统的特殊性，不能简单地将密码学工具应用其中，在保护数据机密性的同时，还要保证系统的实时性和可用性[9]。此外，仅靠上述这些“一对一”的加密手段无法实现云计算环境下数据的灵活访问控制功能，对用户身份的动态变化适应性不够。

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，文献[10]提出了一种属性基加密算法(Attribute-Based Encryption, ABE)。文献[11]又在ABE的基础上提出一种基于密文策略(Ciphertxt-Policy Attribute-Based Encryption, CP-ABE)的加密方案，该方案将访问控制策略嵌入密文之中。在此基础上，Ruj等人[12]第1次在智能电网中使用CP-ABE算法进行访问控制的研究，实现了对用户细粒度的访问控制。之后，Guan等人[13]为实现对智能电网数据的安全采集和高效传输，将大数据分为若干块，并对这些块进行加密/解密和顺序传输，但数据加密前处于离线状态，无法进行实时上传。Das等人[14]则从系统上层框架入手，构建了基于属性的访问控制模型，该模型使用时间、位置、身份等属性，为物联网设备搭建了一个安全的信息共享框架。文献[15]开发了更加具体的方案，利用CP-ABE加密工业物联网数据，构建安全的数据通信方案，保护工业物联网的通信安全。

在上述的标准CP-ABE方案中，密文长度随着访问策略的复杂度而增加，用户在解密过程中需运行的双线性对运算、指数运算的次数也随之增加，从而一方面导致用户端的解密开销增大，另一方面需要用户提供更大的存储空间。为此，Doshi等人[16]从密文长度恒定这一角度入手，提出了一种密文定长的CP-ABE算法，减小了用户的存储及解密开销，与标准方案相比实用性更好。与之类似，王建华等人[17]也提出一种定长CP-ABE方案，具有更短的密文长度，并且解密成本为常数。除密文定长外，也有学者采用了计算外包的方法来降低用户端解密开销。Qin等人[18]设计了一种支持数据验证的解密外包方案，首先将大部分解密运算外包给第三方，减轻了用户端的开销，再通过计算合并密文和密钥后的散列值的方法来验证数据的完整性。与之类似，Yang等人[19]将这种思想应用在医疗物联网环境，构建了轻量级的数据共享系统。但是文献[18]、文献[19]两种方案均未实现密文长度恒定的功能。

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的特点，设计了一种适用于工业控制系统的数据加密传输方案。本文方案在保护数据机密性的同时，还支持灵活的访问控制功能，有效地控制了用户权限，保护了数据隐私。本文方案采用了混合加密的方法，即先用AES算法加密工业数据，再用CP-ABE算法加密AES密钥，以此获得较短的加密时间与较高的安全性。此外，本文方案一方面将密文长度定长，另一方面将大部分解密过程外包，以此来减小用户端的存储与解密开销。同时，为应对存储数据损坏、篡改和回滚攻击等状况的发生，方案还验证了数据完整性和密钥正确性。最后，从方案的正确性、安全性和性能开销3个方面进行分析，并给出仿真结果。

2　预备知识

2.1　双线性配对

设G_1和G_2是两个阶为素数p的循环群，g是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) 双线性性：对任意的$a,b\in Z_p$，满足$e\left(g^a,g^b\right)=e(g,g)^{ab}$；

(2) 非退化性：存在$g\in G_1$，使得$e(g,g)\neq 1$；

(3) 可计算性：对任意$\forall(u,v)\in G_1$，都能有效计算出$e(u,v)$。

2.2　系统模型

本文构造的系统模型如图1所示，系统模型由授权中心，工业控制系统，私有云，公有云，和数据用户5个实体构成，实体间的算法关系将在下一节中详细阐述，现对每个实体的主要功能总结如下：

(1) 授权中心(Key Generation Center, KGC)：KGC是一个独立且可信任的机构，具有为新用户授权和分配全局标识符GID(Global IDentifier, GID)的权限。同时，KGC主要计算系统公共参数、系统主密钥对和属性私钥sk_L。

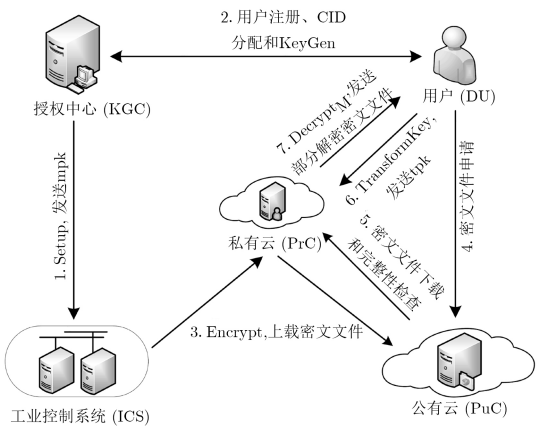

图 1 系统模型图

(2) 数据用户(Data User, DU)：企业内需要读取现场数据的工作人员(包括经理、工程师等)。为保护数据安全，新用户在进入系统前，需向KGC申请注册，获得合法且唯一的GID和属性私钥。在计算转换密钥时，用户则使用属性私钥和GID计算转换密钥对。

(3) 私有云(Private Cloud, PrC)：企业为其单独使用而构建的私有云平台，在平台上部署相关应用程序，能够获得对数据、安全性和服务质量的最有效控制，但不能进行大规模的数据存储。在此模型中，私有云负责外包解密计算和数据完整性检查服务。

(4) 公有云(Public Cloud, PuC)：第三方为企业提供的一个半可信云平台，没有访问密文的权限，但企业可在PuC上进行数据存储、资源托管等服务。在此模型中，只有当PuC接收到DU提出的密文申请后，才能将密文文件发给PrC。

(5) 工业控制系统(Industrial Control System, ICS)：企业内对现场设备进行监控，并采集现场数据(包括设备状态参数，工艺参数，现场环境数据等)的系统。本模型中，ICS先用对称加密算法(AES)加密采集到的数据，形成数据密文AES(M,DATA)，再用CP-ABE算法加密对称密钥M，形成密钥密文CT，最后将数据密文及密钥密文按照一定的格式上传至公有云存储。为保护ICS的安全，ICS不能直接与外网的公有云连接，密文文件需先上传至私有云，再转发至公有云存储。

3 系统方案

3.1 系统方案构造

为保障工控系统中数据的安全传输，结合工业控制系统的实时性、可靠性及资源有限的特点，本文在文献[16]算法的基础上设计出一种适用于工控系统的加密传输方案，其主要包含6个基本算法：Setup, Encrypt, KeyGen, TransformKey, Decrypt$_{M'}$和Decrypt。

假设方案中$U=\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_n\}$是一个属性集合，$S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$是属性$\mathrm{att}_i$所有可能的属性值，$n_i$是属性值的最大个数，$L=\{L_1,L_2,\cdots,L_n\}$是用户的属性集合，$W=\{W_1,W_2,\cdots,W_k\}$是访问结构。方案构造过程如下：

(1) $\mathrm{Setup}(\lambda)\to\{\mathrm{PP},\mathrm{mpk},\mathrm{msk}\}$：由授权中心(KGC)运行。KGC首先计算公开参数PP，定义两个阶为素数p的乘法循环群(G_1,G_T)，$e:G_1\times G_1\to G_T$是一对双线性映射，$H:\{0,1\}^*\to G_1$和$H_1:\{0,1\}^*\to Z_p$分别是两个抗碰撞的哈希函数，$g,u\in G_1$。计算的系统公开参数PP是

$$\mathrm{PP}=\{G_1,G_T,H,e,g,u\} \tag{1}$$

然后，KGC再计算系统主密钥对。授权中心为拥有权限的用户分配一个独一无二的全局标识符GID，再为用户的每个属性$\mathrm{att}_i\in U$选择两个随机数$\alpha_{i,j}\in Z_{P(i\in[1,n],j\in[1,n_i])}$和$t\in Z_P$，计算出$Y=e(g,g)^t$和$T_{i,j}=g^{-\alpha_{i,j}}$，最后，生成的系统主密钥对$(\mathrm{mpk},\mathrm{msk})$为

$$\begin{aligned}\mathrm{msk}&=\left(t,\alpha_{i,j}\left(i\in[1,n],j\in[1,n_i]\right)\right),\\ \mathrm{mpk}&=\left(Y,T_{i,j}\left(i\in[1,n],j\in[1,n_i]\right)\right)\end{aligned} \tag{2}$$

(2) $\mathrm{KeyGen}(\mathrm{msk},L)\to\{\mathrm{sk}_L\}$:由授权中心(KGC)运行。由DU先向KGC申请属性私钥，算法输入属性权威私钥msk，用户属性列表L，计算出用户私钥sk_L

$$\begin{aligned}\mathrm{sk}_L=\Bigg\{&\mathrm{sk}_1=g^{\alpha_{i,j}}H(\mathrm{GID})^{\alpha_{i,j}}\big|_{v_{i,j}\in L},\\ &\mathrm{sk}_2=g^t\left(\prod_{v_{i,j}\in L}g^{\alpha_{i,j}}\big|_{v_{i,j}\in L}\right)\Bigg\}\end{aligned} \tag{3}$$

(3) $\mathrm{Encrypt}(M,\mathrm{mpk},W)\to\{\mathrm{CT}\}$：由工业控制系统(ICS)运行。算法输入属性权威公钥mpk、用户访问结构W、密钥M $(M\in Z_P)$和一个随机值$s\in Z_P$，最后计算密钥验证码V，得到的密钥密文CT为

$$\begin{aligned}\mathrm{CT}=\Bigg\{&C_0=M\mathrm{Y}^s,C_1=\left(\prod_{v_{i,j}\in W}T_{i,j}\right)^s,\\ &C_2=g^s,V=H_1\left(u^M\right)\Bigg\}\end{aligned} \tag{4}$$

(4) $\mathrm{TransformKey}(\mathrm{sk}_L,\mathrm{GID})\to\{\mathrm{tk}_{\mathrm{GID}}\}$：由数据用户(DU)运行。DU选择一个随机值$z\in Z_P$和属性私钥$\mathrm{sk}_L$，根据用户GID，生成的转换密钥$\mathrm{tk}_{\mathrm{GID}}$为

$$\begin{aligned}\mathrm{tk}_{\mathrm{GID}}=\Bigg\{&\mathrm{tpk}_{i,j}=\left(\mathrm{sk}_1^{\frac{1}{z}},\mathrm{sk}_2^{\frac{1}{z}},H(\mathrm{GID})^{\frac{1}{z}}\right)_{v_{i,j}\in L},\\ &\mathrm{tsk}_{\mathrm{GID}}=z\Bigg\}\end{aligned} \tag{5}$$

(5) $\mathrm{Decrypt}_{M'}(\mathrm{tpk}_{i,j},L)\to\{M'\}$：由私有云(PrC)运行。PrC按照事先约定的文件传输格式取出密文CT，再对CT进行部分解密。若属性列表L满足密文访问策略W(即$L\models W$), PrC能够成功进行部分解密计算；相反，PrC解密失败并输出$\perp$。解密过程

$$M'=\frac{e\left(C_2,\mathrm{sk}_2^{\frac{1}{z}}\right)}{e\left(C_2,\prod\limits_{v_{i,j}\in L}\mathrm{sk}_1^{\frac{1}{z}}\right)e\left(C_1,H(\mathrm{GID})^{\frac{1}{z}}\right)} \tag{6}$$

解密得到部分密文为：$M'=e(g,g)^{\frac{\mathrm{st}}{z}}$。最后，PrC将$M'$和AES$(M,\mathrm{DATA})$发送给DU。

(6) Decrypt$(M',\mathrm{tsk}_{\mathrm{GID}})\to\{M\}$：由数据用户(DU)运行。DU收到$M'$后，只需进行一次简单的指数运算即可得到对称加密密钥M，再使用密钥M解密AES(M,DATA)就可以获得现场数据。解密过程包括如下两个步骤：

(a) DU先进行一次指数运算得到M，解密过程为

$$M=\frac{C_0}{(M')^{\mathrm{tsk}_{\mathrm{GID}}}} \tag{7}$$

(b) 然后进行密钥验证和AES解密。DU先计算密钥验证码$H_1\left(u^M\right)$，如果$H_1\left(u^M\right)=V$，表明密钥是正确的，DU可使用密钥M对AES(M,DATA)进行解密，得到现场数据DATA；否则，立即停止计算。

3.2 数据完整性检查

使用加密的方式能够保护存储在公有云中数据的机密性，却无法保证由于配置错误造成数据损坏、篡改等情况和数据新鲜度过期。数据新鲜度是指发送到云端的数据始终是最新的，防止出现提供过时数据的回滚攻击。使用数据完整性检查可以实时验证公有云中数据的完整性和新鲜度，当数据不完整或不新鲜时，私有云能及时对数据进行处理。企业使用挑战应答的方式完成部署在公有云中的完整性检查服务，挑战由私有云向公有云发起，公有云通过挑战信息完成应答，私有云则利用应答信息获取存储数据的完整性状况。认证的详细过程如下：

(1)初始化阶段

步骤 1　公有云根据Setup算法生成密钥对$\{g^\alpha,\alpha\}$。

步骤 2　公有云先对密文F分块处理，将其分为$F=\{f_1,f_2,\cdots,f_n\}$，再随机选择$r_i\in Z_P$，为所有数据块计算相应的认证元集合$\Psi=\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$，式中$\lambda_i=(H(i)\cdot u^{r_i})^\alpha$, $H(i)$是哈希运算。

步骤 3　公有云将$\{r_i,\lambda_i\}$附在密文后面发送给私有云。

(2)挑战阶段

步骤 1　私有云作为验证者，对公有云发起周期性的完整性验证。首先从$F=\{f_1,f_2,\cdots,f_n\}$的分块中随机选取t个索引编号，并为每块文件编号选取一个随机数$v_i\in Z_P$，再将编号和随机数组合形成挑战请求$\{i,v_i\}_{i\in[1,n]}$发送至公有云。

步骤 2　公有云利用v_i进行以下计算

$$\eta=\sum_{i=i_1}^{i_t}v_i\cdot r_i,\lambda=\prod_{i=i_1}^{i_t}\lambda_i^{v_i} \tag{8}$$

然后将$\{\eta,\lambda\}$作为应答信息发送给私有云。

步骤 3　私有云接收到$\{\eta,\lambda\}$后，判断等式(9)是否成立，若等式成立，则公有云中存储的数据是完整且可使用的。

$$e(\lambda,g)=e\left(\prod_{i=i_1}^{i_t}H(i)^{v_i}\cdot u^\eta,g^\alpha\right) \tag{9}$$

4　系统方案分析

4.1 机密性分析

本方案采用混合加密方法，即先使用对称加密算法(AES)加密工业数据，再用改进后的文献[16]的CP-ABE算法加密对称密钥M，可见工业数据的机密性主要由数据密文和密钥密文的机密性决定，而数据密文的机密性又取决于密钥密文的机密性。文献[16]的算法已被证明是满足CPA安全，而本算法为文献[16]算法的属性私钥增加了一组用于外包解密的组件，将用户秘密保存的随机值z嵌入到转换密钥的公钥$\mathrm{tpk}_{i,j}$中，令攻击者无法在有效的多项式时间内分离出z值，从而无法成功解密，最终保证了本文法的机密性。

4.2 抗合谋攻击

在工业企业内部，某些没有权限的用户企图通过合谋获得工业数据，当用户进行合谋时，只有正确计算出$e(g,g)^{\frac{\mathrm{st}}{z}}$的值，才能成功解密密钥密文。然而在本算法中，随机值s被嵌入到密文中，随机值t被嵌入到私钥中，合谋者即使获得密文和私钥的组件，也无法分离出s和t。除此之外，在配对计算时还需使用$H(\mathrm{GID})$，但每个用户的GID都是独一无二的，其哈希值$H(\mathrm{GID})$也是唯一的。所以，未授权用户无法通过合谋计算出$e(g,g)^{\frac{\mathrm{st}}{z}}$的值去解密密钥密文，也无法解密数据密文。

4.3 数据完整性

将密文文件存储在公有云中，为应对突然出现的文件损坏、篡改和回滚攻击等状况，本文利用挑战应答的方式对文件进行周期性检查。在挑战应答的过程中，私有云采用双线性映射配对的方式对等式进行有效验证，确保公有云中密文文件的完整性。

为确保对称密钥M是正确可用的，用户需先通过指数运算和哈希运算计算出密钥验证码$H_1\left(u^M\right)$，再采用等式验证的方法检验密钥验证码的正确性。

本文的数据完整性检查方法与文献[18]中用户方先解密再验证的传统方法相比，可持续性地对数据文件实施完整性检查服务，还能够减轻用户端的计算开销，且保证文件内容无法被泄露。

5　性能分析

下面从方案性能、计算开销、通信密文长度这

3个方面将本文案与文献[16]、文献[18]和文献[19]的方案进行比较，最后进行实验并评估方案性能。在分析过程中，$|G_1|$, $|G_T|$和$|Z_P|$分别表示G_1, G_T和Z_P中元素的长度，E_1, E_T分别表示G_1和G_T中的指数运算，P代表配对运算，n表示用户属性数量。

5.1 方案性能比较

如表1所示，本文方案支持外包解密和密文定长，而且还具有对密钥正确性和数据完整性进行验证的功能，确保用户得到的数据和密钥都未遭受过损坏或篡改。

本文方案中，密文长度主要考虑两部分，第1部分是私有云端密文长度，第2部分是用户端密文长度，此处不考虑对称加密密文长度。本文方案在文献[16]的基础上将计算外包至私有云，因此需在用户端存储的密文长度仅为$|G_T|$，优于文献[16]的$4|G_1|$。文献[18]、文献[19]虽也采用了计算外包的方法，但二者密文长度均与属性数量相关，尤其是在文献[18]中，用户端的密文长度随着属性数量的增加而增加。本方案由于将密文定长，因此无论是在私有云还是在用户端所需要的存储消耗均为最小且是一个常数值。

5.2 计算开销

与文献[16]、文献[18]和文献[19]关于计算开销的对比结果如表2所示，此处忽略对称加密和哈希计算的开销。与文献[16]相比，加密开销相差不大，但本文方案的用户解密开销远远小于文献[16]。本文方案和文献[18]、文献[19]都使用外包解密技术，将大量的解密计算外包给第三方，减轻了用户方的计算负担。仅针对计算开销而言，本文方案的计算开销为$3P+2E_1+2E_T$，是一个定值，而文献[18]、文献[19]的计算开销均与属性数量线性相关，文献[18]为$(n+2)P+(2n+1)E_T$，文献[19]为$3P+(2n+8)E_1+E_T$。通过以上分析可见，本文方案在计算开销方面具有明显优势，尤其是用户端的计算开销仅为E_T。

5.3 实验仿真

本节通过仿真验证上述理论分析的计算开销，并评估方案性能。实验采用斯坦福大学开发的双线性对密码库(PBC Library)，椭圆曲线采用Type A: $y^2=x^3+x$，仿真硬件为Inter(R)Core(TM)i5-3470 3.2 GHz CPU, 4.00 GB内存，Windows7 32 bit操作系统，对称加密算法采用的是128 bit AES算法。

从图2可知，本文算法的私钥生成时间随着属性个数增加而增加，但私钥的生成是在独立的授权中心完成的，仅在新用户注册时才运行1次。图3表示本算法的加密时间，可见加密时间与属性数量成正相关关系，但即使属性个数达到100，加密时间也只有58 ms。在图4中，本文算法的解密时间基本恒定，外包解密时间为46 ms，用户解密时间只有2 ms。通过对比外包解密时间和用户解密时间可见，方案将大量的解密开销外包给私有云，用户只需进行少量的有限次运算即可。

5.4 应用场景分析

根据图1设计的系统模型，本文采用VMware和hadoop-2.8.4搭建的工业控制系统云平台如图5所示，云平台中包含有2个用户节点、1个私有云和1个公有云。其中私有云包含2个节点：Ubuntu(KGC), Ubuntu(PrC)，公有云只有1个节点Ubuntu(PuC)，每个节点上都安装了hadoop；用户节点分别为Ubuntu(ICS)和Ubuntu(DU)。在图5中，Ubuntu(KGC), Ubuntu(PuC), Ubuntu(PrC), Ubuntu(ICS)和Ubuntu(DU)分别代表着系统模型中的KGC, PuC, PrC, ICS和DU，并给所有节点都分配了不同的IP地址。

假设应用场景中所有数据都存放在hadoop分布式文件系统(Hadoop Distributed File System, HDFS)上，其流程如下：(1)Ubuntu(KGC)将生成的公钥和私钥组件存储在HDFS1中，当DU和ICS需要组件时KGC会从HDFS1中下载相应组件，如图5中步骤①所示；(2)Ubuntu(ICS)将收集的数据进行加密，并将加密文件由PrC转发至Ubuntu(PuC)存储在HDFS2中，如图5中步骤②所示；(3)DU向PuC发起密文文件申请，Ubuntu(PuC)从HDFS2中将文件下载后再发给Ubuntu(PrC)进行解密计算，如图5中步骤③所示；(4)DU将$\text{tpk}_{i,j}$发给Ubuntu(PrC)进行解密计算，如图5中步骤④所示；(5)Ubuntu(PrC)将部分解密密文发送给Ubuntu(DU)，如图5中步骤⑤所示。

表 1 方案性能比较

方案	是否外包解密	是否密文定长	是否可验证	私有云端密文长度	用户端密文长度
文献[16]	否	是	否	–	$4\|G_1\|$
文献[18]	是	否	对称密钥	$(n+2)\|G_1\|+\|G_T\|$	$(n+2)\|G_1\|$
文献[19]	是	否	密文	$3\|G_1\|+\|G_T\|+2n\|Z_p\|$	$2\|G_T\|$
本文方案	是	是	对称密钥/密文	$2\|G_1\|+\|G_T\|$	$\|G_T\|$

表 2　计算开销比较

方案	加密开销	外包解密开销	用户解密开销
文献[16]	$3E_1+E_T$	–	$3P+nE_1$
文献[18]	$(2n+1)E_1$	$(n+2)P+2nE_T$	E_T
文献[19]	E_1+E_T	$3P+2nE_1$	$7E_1$
本文方案	$2E_1+E_T$	$3P$	E_T

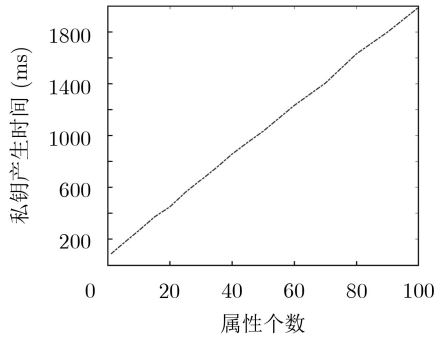

图 2 私钥生成时间

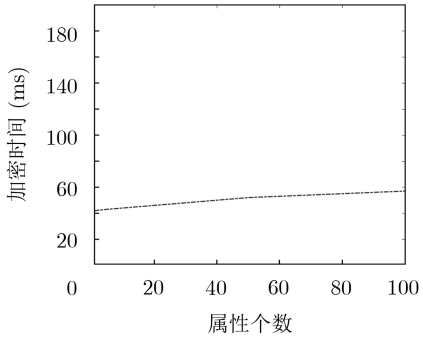

图 3 加密时间

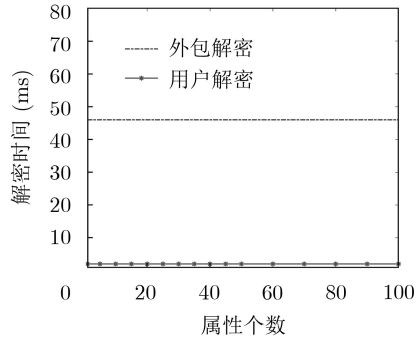

图 4 解密时间

6　结束语

本文采用CP-ABE算法设计了一种适用于工业控制系统的数据加密传输方案，既实现了对工业数据机密性的保护，又获得了细粒度的访问控制。方案不仅支持外包解密，还具有密文长度恒定的特点，因此有效地降低了用户端的密文存储与解密开销。此外，方案中的数据检验功能有效检测了数据

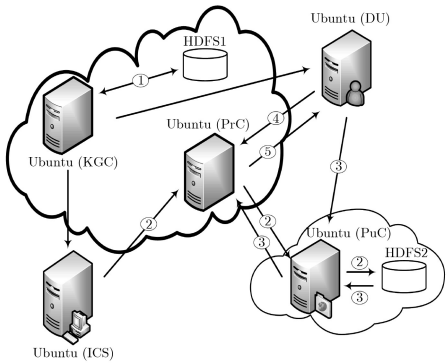

图 5 应用场景

完整性和密钥的正确性。最后，与已有方案进行了比较分析，结果表明本文方案具有低解密开销的性能优势，同时也将方案应用于工业控制系统云平台上，表明本文方案在工业控制系统中具有良好的可适应性。

参 考 文 献

[1] SAJID A, ABBAS H, and SALEEM K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges[J]. *IEEE Access*, 2016, 4: 1375–1384. doi: 10.1109/ACCESS.2016.2549047.

[2] TRAUTMAN L J and ORMEROD P. Industrial cyber vulnerabilities: Lessons from stuxnet and the internet of things[J]. *University of Miami Law Review*, 2017, 72: 761–826. doi: 10.2139/ssrn.2982629.

[3] BABU B, IJYAS T, MUNEER P, *et al*. Security issues in SCADA based industrial control systems[C]. The 2nd International Conference on Anti-Cyber Crimes, Abha, Saudi Arabia, 2017: 47–51. doi: 10.1109/Anti-Cybercrime.2017.7905261.

[4] KRIAA S, PIETRE-CAMBACEDES L, BOUISSOU M, *et al*. A survey of approaches combining safety and security for industrial control systems[J]. *Reliability Engineering & System Safety*, 2015, 139: 156–178. doi: 10.1016/j.ress.2015.02.008.

[5] 周小锋, 陈秀真. 面向工业控制系统的灰色层次信息安全评估模型[J]. 信息网络安全, 2014(1): 15–20. doi: 10.3969/j.issn.1671-1122.2014.01.004.

ZHOU Xiaofeng and CHEN Xiuzhen. Gray analytical hierarchical assessment model for Industry control system security[J]. *Netinfo Security*, 2014(1): 15–20. doi: 10.3969/j.issn.1671-1122.2014.01.004.

[6] HALAS M, BESTAK I, ORGON M, *et al*. Performance measurement of encryption algorithms and their effect on real running in PLC networks[C]. The 35th International Conference on Telecommunications and Signal Processing, Prague, Czech Republic, 2012: 161–164. doi: 10.1109/TSP.

2012.6256273.

[7] LI Xing, LIU Mengxiang, ZHANG Rui, *et al*. Demo abstract: An industrial control system testbed for the encrypted controller[C]. The 9th ACM/IEEE International Conference on Cyber-Physical Systems, Porto, Portugal, 2018: 343–344. doi: 10.1109/ICCPS.2018.00045.

[8] 李兴. 工业控制系统加密控制器实验平台及方法研究[D]. [硕士论文], 浙江大学, 2018.
LI Xing. Industrial control systems testbed and method study of the encrypted controller[D]. [Master dissertation], Zhejiang University, 2018.

[9] CHEMINOD M, DURANTE L, and VALENZANO A. Review of security issues in industrial networks[J]. *IEEE Transactions on Industrial Informatics*, 2013, 9(1): 277–293. doi: 10.1109/tii.2012.2198666.

[10] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

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

[12] RUJ S and NAYAK A. A decentralized security framework for data aggregation and access control in smart grids[J]. *IEEE Transactions on Smart Grid*, 2013, 4(1): 196–205. doi: 10.1109/TSG.2012.2224389.

[13] GUAN Zhitao, LI Jing, WU Longfei, *et al*. Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid[J]. *IEEE Internet of Things Journal*, 2017, 4(6): 1934–1944. doi: 10.1109/JIOT.2017.2690522.

[14] DAS P K, NARAYANAN S, SHARMA N K, *et al*. Context-sensitive policy based security in internet of things[C]. 2016 IEEE International Conference on Smart Computing, Louis, USA, 2016: 1–6. doi: 10.1109/SMARTCOMP.2016.7501684.

[15] CHAUDHARY R, AUJLA G S, GARG S, *et al*. SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(6): 2629–2640. doi: 10.1109/TII.2018.2789442.

[16] DOSHI N and JINWALA D. Constant ciphertext length in CP-ABE[EB/OL]. https: //eprint.iacr.org/2012/500.pdf, 2012.

[17] 王建华, 王光波, 徐旸, 等. 解密成本为常数的具有追踪性的密文策略属性加密方案[J]. 电子与信息学报, 2018, 40(4): 802–810. doi: 10.11999/JEIT170198.
WANG Jianhua, WANG Guangbo, XU Yang, *et al*. Traceable ciphertext-policy attribute-based encryption scheme with constant decryption costs[J]. *Journal of Electronics & Information Technology*, 2018, 40(4): 802–810. doi: 10.11999/JEIT170198.

[18] QIN Baodong, DENG R H, LIU Shengli, *et al*. Attribute-based encryption with efficient verifiable outsourced decryption[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(7): 1384–1393. doi: 10.1109/TIFS.2015.2410137.

[19] YANG Yang, LIU Ximeng, and DENG R H. Lightweight break-glass access control system for healthcare internet-of-things[J]. *IEEE Transactions on Industrial Informatics*, 2017, 14(8): 3610–3617. doi: 10.1109/TII.2017.2751640.

屠袁飞：男，1984年生，博士生，工程师，主要研究方向为网络安全、云计算与访问控制.

苏清健：男，1994年生，硕士生，主要研究方向为云计算与访问控制.

杨 庚：男，1961年生，博士，教授，博士生导师，主要研究方向为网络安全、分布式与并行计算等.