计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20180217
56(5):1112-1122,2019

轻量级窄带物联网应用系统中高效可验证加密方案

钱涵佳[1] 王宜怀[1,2] 彭 涛[1] 陈 成[1] 罗喜召[1]
[1](苏州大学计算机科学与技术学院 江苏苏州 215006)
[2](苏州市嵌入式技术及应用重点实验室(苏州大学) 江苏苏州 215006)
(20164227026@stu.suda.edu.cn)

Efficient and Verifiable Encryption Scheme in Lightweight Narrowband Internet of Things Applications

Qian Hanjia[1], Wang Yihuai[1,2], Peng Tao[1], Chen Cheng[1], and Luo Xizhao[1]
[1](*College of Computer Science and Technology, Soochow University, Suzhou, Jiangsu* 215006)
[2](*Suzhou Municipal Key Laboratory of Embedded Technology and Applications* (*Soochow University*), *Suzhou, Jiangsu* 215006)

Abstract Narrowband Internet of things (NB-IoT) is an important branch of the Internet. It can provide application-level services and achieve information intellectualization, relying on the powerful resource processing capability offered by cloud computing. However, due to the storage of data in different places, cloud platform service providers are not completely trusted. User data is exposed in a not completely secured environment and this brings many security problems, such as external malicious attack and cloud server collusion. Aiming at these NB-IoT's issues like its terminal nodes are vulnerable to attacks, lacking in resources, limit in power consumption, a property-based cloud storage fast access control scheme is proposed. Under the background of multiple attribute authorities, an efficient and verifiable lightweight cryptographic encryption schemes is the goal. So using the idea of online/offline encryption and combining outsourced decryption technology, an online/offline and outsourced multi-authority ciphertext-policy attribute-based encryption scheme (OO-MA-CP-ABE) which can be secured from chosen-plaintext attack (CPA) is constructed. It improves the efficiency of the encryption and decryption algorithm while minimizing user's computational overhead, quite suitable for terminal equipment with weak computing power and limited resources, and can further ensure the correctness of outsourced computing by verifying the algorithm as well. It also gives the security analysis of the lightweight NB-IoT application system under cloud computing environment, in order to ensure the flexible and extensible access control strategy and the confidentiality and privacy protection of user data during the resource sharing process. Finally, the performance analysis of the OO-MA-CP-ABE scheme is given, and compared with the existing schemes in terms of functionality, computational overhead and storage overhead.

Key words narrowband Internet of things; multiple authorized institutions; privacy protection; online/offline encryption; outsourcing decryption

收稿日期:2018-04-01;**修回日期**:2018-08-14
基金项目:国家自然科学基金项目(61672369)
This work was supported by the National Natural Science Foundation of China (61672369).

摘 要 窄带物联网(narrowband Internet of things, NB-IoT)是互联网中的一个重要分支.NB-IoT 依托云计算强大的资源处理能力提供应用层的各项服务以及实现信息智能化.然而由于数据异地存储,云平台服务提供商并不完全可信,用户数据暴露在不完全安全的环境下,带来了诸多安全问题,比如被外部用户恶意攻击、云服务器共谋攻击等.针对 NB-IoT 终端节点极易受到攻击、资源不足、功耗受限等问题,提出一种基于属性的云存储快速访问控制方案.在多个属性授权机构的背景下,以高效可验证的轻量级加密方案为目标,借鉴在线/离线加密思想,并结合外包解密技术,构造了具备选择明文攻击(chosen-plaintext attack, CPA)安全的在线/离线加密和外包解密的多机构密文策略属性基加密方案(online/offline and outsourced multi-authority ciphertext-policy attribute-based encryptin scheme, OO-MA-CP-ABE),提高加解密算法效率的同时最小化用户的计算开销,很适合计算能力弱且资源受限的终端设备.并进一步通过验证算法确保外包计算的正确性.还给出了云计算环境下轻量级 NB-IoT 应用系统安全性分析,保证资源共享过程中,灵活可扩展的访问控制策略以及用户数据的机密性和隐私保护.最后,给出了 OO-MA-CP-ABE 方案的性能分析,从功能性、计算开销和通信开销 3 个方面同现有方案进行比较.

关键词 窄带物联网;多授权机构;隐私保护;在线/离线加密;外包解密

中图法分类号 TP309

基于蜂窝的窄带物联网(narrowband Internet of things, NB-IoT)是第 3 代合作伙伴计划(3rd Generation Partnership Project, 3GPP)标准组织于 2015 年 9 月定义的面向低功耗广域网(low power wide area network, LPWA)的关键蜂窝网络通信技术[1].2016 年 6 月 16 日,3GPP 标准组织在韩国釜山正式确立了 NB-IoT 系列标准核心协议[2].

NB-IoT 技术本身具备低功耗、低成本、广覆盖、深穿透、大连接等优势[3],填补了 LPWA 市场中无法大规模、长距离、广部署的技术空白,完美匹配了低功耗广覆盖的物联网市场需求.因此,该技术吸引了国内外主流运营商、设备厂商的加入,正以一种势不可挡的态势发展.成为物联网主流技术之一,被广泛应用于多种垂直行业,如远程抄表、智能家居、环境监测、智能农业、资产跟踪等.

在 NB-IoT 应用推广中,其必须建立开放产业平台,依托云计算这个拥有强大计算存储能力的大数据处理支撑平台,提供 NB-IoT 应用层的各项数据服务以及实现信息智能化.然而,云计算环境下数据存储安全存在问题.由于数据异地的存储,导致用户失去对自身数据的一些基本访问控制.云环境的开放性对用户而言不可完全信赖,用户数据将会暴露在不安全的云环境之下,容易受到恶意外部攻击者、内部员工隐瞒窃探和云服务器共谋攻击等威胁,数据机密性和用户隐私难以得到保证,此外,由于 NB-IoT 感知层由海量智能化程度受限的终端节点组成,不具备自我保护措施,并且由于窄带物联网是开放性网络,资源提供方容易受到节点冒充、数据篡改、信息窃取等攻击.在数据处理共享需求越来越多的分布式环境中,如何在灵活可扩展的访问控制策略下,控制数据共享范围的同时,也保障用户在通信过程中数据的机密性、隐私性是一个严峻的挑战[4-5].

加密技术是目前保证物联网数据传输以及云储存共享安全性应用最为广泛的技术,也是访问控制策略模型实现的基础.大规模 NB-IoT 分布式应用中设计可靠的加密方案必须考虑 3 个问题:1)细粒度访问控制.NB-IoT 拥有大量用户,需要根据用户级别设定权限访问,增加访问策略的灵活性,更易描述区分访问用的权限,控制数据共享访问的范畴,让用户受控进行数据分享.2)用户数据安全隐私保护.在分布式应用中,隐藏用户身份信息,保护云存储数据机密性和访问控制策略.3)系统效率及开销.考虑到大规模分布式应用中一对多的通信模式,降低为每个用户加密数据的花销.NB-IoT 感知层中的节点计算能力有限,电池容量较低,这就要求尽量降低整个方案尤其是终端节点的计算、存储开销.寻找适于物联网、云存储的轻量级加密算法.基于属性的加密技术(attribute based encryption, ABE)可以很好地应用于细粒度访问控制中,能有效地实现分布式环境下灵活可靠的数据共享.保证数据安全和用户隐私,并且将计算密集型任务外包到云代理上,降低因为加解密算法给物资受限的 NB-IoT 终端设备的计算开销,从而可以改善设备电池寿命.基于属性的加密算法前身是基于身份的加密技术(identity based

encryption, IBE). 在 1984 年 Shamir[6] 在公钥基础设施以及双线性对的基础上建立了 IBE 方案,其中将用户身份信息作为用户的公共密钥,由加密方自己保存私钥,那么加密方无需事先在线获得解密方的真正数字公钥证书(证书中存取公共密钥)就可以实现加密. 该方案不仅解决了基于证书的公钥加密体制中的一大缺陷,还很好地简化了加密过程,节省了很大的加密开支.

在实际应用中,IBE 加密体制需要庞大的存储空间和计算量,也无法抵抗多个用户合谋伪造身份的联合攻击. 基于此,Sahai 和 Waters[7] 给出了一种新的加密方案——模糊的基于身份的加密方式(fuzzy IBE),首次提出了用一组属性的集合来描述身份的概念. 在 fuzzy IBE 的基础上,ABE 加密体制进一步被提出,实现用一组可以描述用户身份的属性集合来进行加解密的方案. 由于基本 ABE 无法支持灵活的访问控制策略,访问控制策略树的概念随即被提出,由此衍生出了 2 种基于策略树的 ABE 加密算法. 一种是 Goyal 等人[8] 提出的基于密钥策略的 ABE(key-policy ABE, KP-ABE)和 Bethencourt 等人[9] 提出的基于密文策略的 ABE(ciphertext-policy ABE, CP-ABE).

在 KP-ABE 中,使用树形访问结构来控制权限,访问结构关联在用户私钥中,属性关联密文,只有当密文属性满足访问结构时,用户才能使用私钥解密密文恢复出明文. 该方案下,加密方完全无法控制明文,适合应用于大规模下网络环境中的密钥管理.

CP-ABE 类似于广播加密,无需加密方考虑解密者的身份问题,适用于分布式网络,与 KP-ABE 相同的是,其也运用访问控制结构来控制权限并由发送方指定,与生成的密文相关联,解密密钥用一组可描述的属性集合来约束. 仅当用户属性满足访问策略时,才能获得解密密钥,访问资源. 相较于 KP-ABE,CP-ABE 更适用于物联网安全方案中.

以上方案都是依靠单授权中心识别用户属性,实现系统中每个用户私钥的管理分发. 随着大规模云服务应用中用户数量的不断增加,单授权中心管理分发密钥以及管理用户属性所需的开销急剧增加,容易造成系统崩溃. 2007 年 Chase[10] 提出多个授权中心的 ABE 加密(multi-asuthority ABE, MA-ABE)方案,由多个授权机构分管用户不同属性并生成相应用户属性的私钥. 该方案很好地降低了单授权机构的计算负担. 随后,2012 年马丹丹等人[11] 提出了基于多个授权机构的 CP-ABE 机制,采用访问树结构通过植入随机化参数有效地抵抗了合谋攻击. 因此,MA-ABE 机制更适用于云计算环境中的分布式应用系统. 然而上述方案的时间复杂度较高,有大量双线性配对和幂乘运算,计算复杂度相当高. 另外加解密计算开销与属性个数和访问结构复杂度成线性增关系,导致用户端计算负担较重,不适用于资源受限且计算能力较弱的 NB-IoT 终端设备. 虽然,2014 年 Hohenberger 等人[12] 为了降低加密过程中的计算开销、提高加密效率,构造了在线/离线加密的 CP-ABE 方案. 该方案主要思想是在离线阶段对复杂计算进行预处理,在线阶段仅需执行常数级别的指数操作即可生成密文. Green 等人[13] 提出的密钥转换技术,将 ABE 解密过程中配对操作等复杂运算外包给云服务 ,在不泄露任何的明文信息的前提下,大大减少用户解密花销. 然而该方案只考虑了解密阶段的计算开销,并没有降低用户加密阶段的计算负担. 此外大多数现有的 ABE 方案在构造过程中并没有考虑到外包计算正确性的验证. 基于以上思想,本文在多属性授权机构的背景下,结合在线/离线加密技术和外包解密技术,提出一种新的轻量级窄带物联网应用系统中高效可验证的加密方案.

在本文中,我们提出了基于标准模型下选择明文攻击(chosen-plaintext attack, CPA)安全的在线/离线加密和外包解密的多机构 CP-ABE 加密方案(online/offline and outsourced multi-authority ciphertext-policy ABE scheme, OO-MA-CP-ABE). 该方案具有快速加密和外包解密的特性,大大减少了数据拥有者和数据用户在分布式云计算环境中的计算开销,对于多权限 NB-IoT 应用系统中资源有限的设备来说是非常合适的. 此外,我们还通过将身份标识符直接嵌入用户私钥的构造方式,防止恶意用户的共谋攻击. 在加密阶段,我们构造了一个简单的验证令牌,用于外包计算正确性验证,增强方案的可靠性.

我们的主要贡献有 3 个方面:

1) 首次将快速在线/离线加密和外包解密的多授权机构 ABE 方案应用于轻量级窄带物联网应用系统中,并且利用一种新的验证外包计算正确性的方式,提高了整体方案的可靠性.

2) 采用多属性授权机构,访问策略更灵活的同时减轻了授权中心的负担和风险. 另外通过身份标识直接嵌入用户私钥构造的方式,实现方案的抗共谋性.

3) 在我们的方案中,加密阶段进行的最昂贵的计算可以离线执行,而在线阶段只需要计算一个常数级别的指数操作.在解密期间,代理服务器可以在数据用户提供的转换密钥的帮助下执行部分解密.因此,数据用户只需执行简单的求幂计算操作,省去了大量求解双线性对的计算开销.相比于现有的MA-ABE方案,我们的方案大大减轻了用户的计算和存储负荷.

实验证明本文方案非常适用于解决计算能力弱且资源受限的NB-IoT应用系统中云存储数据安全问题,并给出了安全性证明,表明本文方案具有CPA安全性.从功能性、通信开销和计算开销3个方面对比分析,本文方案优于现有方案,并通过性能分析,表明本方案的高效性.另外密钥存储在云端,大大降低了访问过程中数据通信开销.

1 预备知识

1.1 双线性配对(bilinear pairing)

设阶为大素数 p 的2个乘法循环群 G 和 G_T,其中 g 为群 G 的生成元.双线性配对 $e:G\times G\rightarrow G_T$ 具有3个性质.

1) 双线性.对于 $\forall P_1,P_2,Q_1,Q_2\in G$ 都有:

$$e(P_1+P_2,Q_1)=e(P_1,Q_1)e(P_2,Q_1),$$

$$e(P_1,Q_1+Q_2)=e(P_1,Q_1)e(P_1,Q_2).$$

2) 非退化性.存在 P,Q 属于 G 使得 $e(P,Q)\neq 1$.

3) 可计算性.对 $\forall P,Q\in G$ 存在一个高效的算法可以计算双线性配对 $e:G\times G\rightarrow G_T$ 即 $e(P,Q)$.

1.2 线性秘密分享方案(linear secret sharing scheme, LSSS)

线性秘密分享方案[14]是由秘密持有方将秘密分发给不同用户,只有符合某种标准的用户才有权限重建获得秘密.

LSSS中 U 表示属性空间,p 为素数,一个定义在 U 上的线性秘密共享方案 Π 指:

1) 所有实体共享 $\mathbb{Z}_p$ 上的一个向量.

2) 对于 U 上的每一个访问控制策略 $\boldsymbol{A}$,存在一个 $l\times n$ 的共享矩阵 $\boldsymbol{M}$,对 $i=1,2,\cdots,l$,定义一个从矩阵的第 i 行到属性空间 U 的函数 ρ.随机选取向量 $\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)$,其中,$s,y_2,y_3,\cdots,y_n\in\mathbb{Z}_p$,$s$ 是共享的秘密,则 $(\lambda_1,\lambda_2,\cdots,\lambda_l)^{\mathrm{T}}=\boldsymbol{Mv}$ 是利用线性分享方案得到的关于 s 的 l 个共享组成的向量.对于授权属性集合 I,能在多项式时间内找到 $\{\omega_i\}_{i\in I}$,满足 $\sum_{i\in I}M_i\omega_i=(1,0,\cdots,0)$,则有 $\sum_{i\in I}\lambda_i\omega_i=s$.对于非授权用户,不存在这样的 $\{\omega_i\}_{i\in I}$.

Shamirs[6]门限秘密共享方案是一种典型的秘密共享方案.在该方案中,秘密和秘密分享都是有限域中的元素.秘密持有方会通过有限域随机建立一个 $t-1$ 度多项式来分享秘密值 s.该多项式的系数都是从有限域中随机选取的,而常数项的值为被分享的秘密值 s.被分享的每一部分将成为该多项式上的一点 $(a_i,f(a_i))$.

1.3 l-BDHI困难问题

设阶为大素数 p 的2个乘法循环群 G 和 G_T,其中 g 为群 G 的生成元.双线性配对 $e:G\times G\rightarrow G_T$,基于其判定性 l-BDHI问题是:$\forall\alpha\in\mathbb{Z}_p$ 以及给定 $l+1$ 元组 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l})$ 并判断 G_T 上的随机元素 T 是否等于 $e(g,g)^{1/\alpha}$.如果敌手 A 在多项式时间内能破解 l-BDHI问题的概率是可忽略的,即可证明 l-BDHI问题是困难的.

2 系统模型及安全模型

2.1 系统模型

本文构建的系统模型如图1所示,包含6个部分:数据属主、云服务提供商、数据访问用户、中央授权机构、属性授权机构和云代理服务器.

1) 数据属主(data owner, DO)

数据属主将自身数据加密之后上传至云服务器进行存储分享,同时在密文上指定访问策略并为每个密文生成相应的验证令牌.DO将在空闲时段进行离线加密,预先处理一些复杂计算,生成中间密文 IT(intermediate ciphertext);在线加密时,将完整的密文 CT(complete ciphertext)上传至云存储服务器上.

2) 云服务提供商(cloud service provicer, CSP)

云服务提供商将会提供密文及验证令牌存储和密钥管理的功能,以及数据访问控制服务.但是云服务器是不完全可信的第三方机构.

3) 数据访问用户(data user, DU)

用户与云存储服务器交互,属性授权机构会根据其一组属性值为其分配一组解密密钥.每一个数据共享用户都有唯一的身份标识 GID(global identity),通过云代理服务器帮助解密密文.只有满足访问控制策略的数据共享用户才能完成解密,获得明文并验证解密结果.

4) 属性授权机构(attribute authorities, AA)

属性授权机构 AA 是独立可信的第三方属性权威机构. 在其范围内,负责用户属性的管理分发、撤销和更新任务,多个授权机构根据用户相关属性生成相应的公开密钥和解密密钥. DU 将凭借其全局身份标识 GID 获取一组属性值以及符合其属性值的解密密钥.

5) 中央授权机构(central attribute authorities, CA)

中央授权机构 CA 为完全可信的权威认证机构. 由 CA 建立系统并负责 AA 注册和用户注册,为 AA 及系统中每一个合法用户分配一个全局唯一的身份标识,同时定义系统全局参数. 但不参与任何用户属性管理和属性私钥分发.

6) 云代理服务器(proxy server, PS)

云代理服务器接收用户请求,使用转换密钥完成对密文的部分解密后发给用户. 在不向 PS 泄露任何加密信息的前提下很好地降低了终端用户设备解密的负担. PS 是半可信的,它会尝试解密文件,但不会影响数据的正确性.

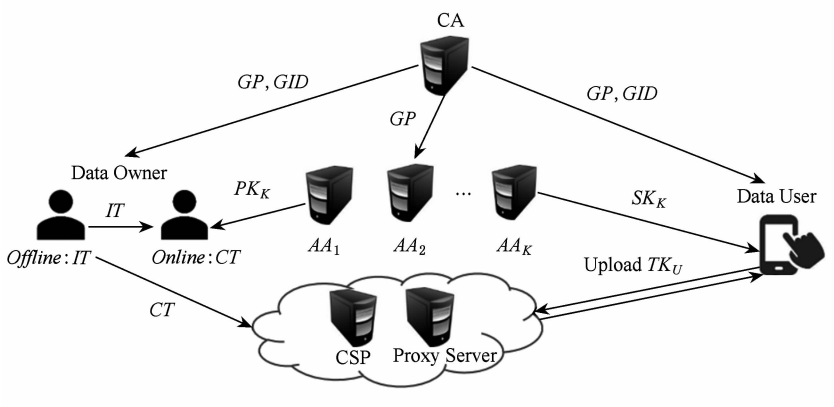

Fig. 1 System model

图 1 系统模型图

2.2 方案定义

在本节中,我们定义本文轻量级窄带物联网应用系统中高效可验证的加密方案多项式时间算法:

1) $CA\_Setup(\lambda, U) \rightarrow GP$

输入安全系数 λ 和属性全集 U,输出系统公开参数 GP(global public parameter). GP 是整个系统方案的全局参数,作为每个算法的输入参数. 假设方案中存在 k 个属性机构 $\{A_1, A_2, \cdots, A_k\}$,每个属性授权机构 A_k 管理相应的一组属性集合 U_k,每个用户拥有全局唯一标识符 GID 以及一组属性集合 S.

2) $AA\_Setup(GP) \rightarrow (PK_k, SK_k)$

属性授权机构初始化时,将 GP 作为输入参数,每个属性授权机构 A_k 生成相应的公私钥对 PK_k, SK_k 作为该算法的输出.

3) $KeyGen(SK_k, GP, S, GID) \rightarrow SK_U$

用户密钥生成算法,由多个授权机构 A_k 合作生成密钥,输入全局参数 GP、授权机构主私钥 SK_k 和一组用户属性集 S,输出每个用户的私钥 SK_U.

4) $Offline.Enc(GP) \rightarrow IT$

离线加密算法,输入全局参数 GP,输出临时密文 IT.

5) $Online.Enc(IT, m, GP, PK_k, (\boldsymbol{M}, \rho)) \rightarrow (CT, Token)$

在线加密算法:输入 GP、属性授权机构主公钥 PK_k、临时密文 IT 访问结构 $(\boldsymbol{M}, \rho)$ 和明文 m(message),输出密文 CT 和验证令牌 $Token$(verification token).

6) $GenToken(SK_U, GP, S) \rightarrow (TK_U, Key)$

转换密钥算法,输入 GP、SK_U 和用户属性集合 S,输出转换密钥 TK_U 和用户秘钥 Key.

7) $Out.Decrypt(GID, GP, CT, TK_U) \rightarrow CT'$

外包部分解密算法由云代理服务器执行. 输入用户 GID、GP、转换密钥 TK_U 和密文 CT,输出部分分解密文 CT'.

8) $Decrypt(CT', GP, Key) \rightarrow m$

用户解密算法:输入用户私钥 Key 和外包密文 CT'、全局公开参数 GP、输出明文消息 m.

2.3 安全模型

我们通过下面的一场攻击游戏来设计本文轻量级窄带物联网应用系统中高效可验证的加密方案的安全模型. 其中,A 为敌手 C 的挑战者,I 代表本文模型中的所有属性授权机构集合[15].

初始化:敌手 A 指定将要被挑战的访问结构 $(\boldsymbol{M},\rho)$以及假冒的属性机构集合 $I'\subseteq I$ 给挑战者 C.

建立:挑战者 C 执行 CA_Setup 算法,产生公共参数 GP,然后将 GP 交给敌手.

对于在 $I-I'$ 中的非假冒授权机构,挑战者 C 会通过执行 AA_Setup 算法生成相应的主公私钥对 (PK_k,SK_k)并发送给 A.

阶段 1:敌手 A 选择一组用户 GID 和用户属性集合 S. 而后挑战者 C 多次提交(S,GID)进行密钥询问. 注意:S 中的每一个属性都不满足访问结构 $(\boldsymbol{M},\rho)$,并且来自于可靠的属性授权机构. C 执行 $KeyGen$ 算法,产生用户私钥 SK_U 发送给敌手 A.

挑战:敌手 A 制定 2 个等长明文消息,M_0,M_1 给挑战者 C;C 选择一个随机值 $b\in\{0,1\}$,执行加密算法产生挑战密文 CT,最后将 CT 发送给敌手 A.

阶段 2:重复阶段 1 的操作.

猜想:敌手输出 b 的猜测值 $b'\in\{0,1\}$. $\exists b=b'$,则敌手 A 获胜.

这里定义敌手 A 的优势为 $Pr[b=b']-1/2$,其成功概率为 $Pr[b=b']$.

定义 1. 如果任意敌手 A 在上述攻击游戏中,在多项式时间内能获胜的概率是可忽略的,那么本方案是 CPA 安全的.

3 方案构建

3.1 NB-IoT 应用架构

从技术科学角度分析,NB-IoT 应用架构可以抽象为 NB-IoT 终端(ultimate-equipment, UE)、NB-IoT 信息邮局(message post office, MPO)、NB-IoT 人机交互系统(human-computer interaction system, HCI)3 个组成部分,如图 2 所示:

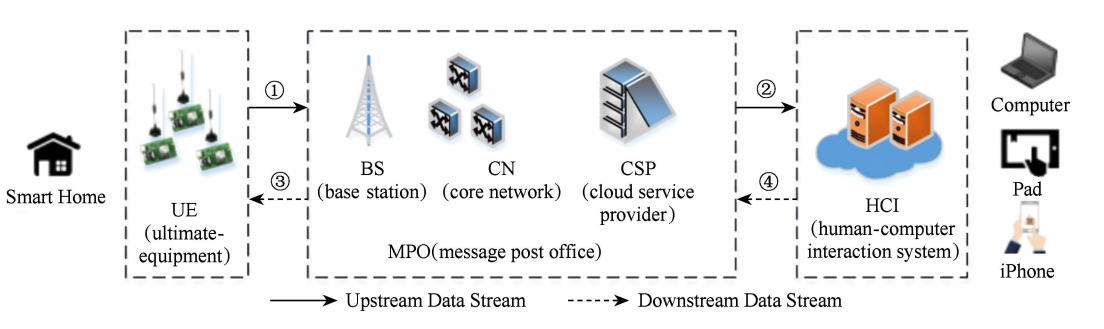

Fig. 2 NB-IoT application architecture

图 2 NB-IoT 应用架构

UE 是以微控制器(microcontroller unit, MCU)为核心,具有 NB-IoT 通信、数据采集、控制、运算等功能的软硬件实体,如燃气表、水表等. MPO 是一种基于 NB-IoT 协议的信息传送系统,是 NB-IoT 基站(base station, BS)、核心网(core network, CN)和设备管理平台(device management server)的总称,是 UE 与 HCI 信息交互的媒介. HCI 是实现具体应用功能的软硬件系统,使人们能够利用通用计算机(PC)、平板电脑、手机等设备实现对例如智能家居、物流等控制的功能. 图 2 中数据传输过程①和②表示上行数据传输过程,③和④代表下行数据传输过程,其中过程①和③使用的是 NB-IoT 协议.

从应用开发的角度来看,开发者只需要对 UE 和 HCI 端的软硬件进行设计. 而对于数据是如何在 MPO 内部传输的这个问题将由运营商解决. 所以开发者在进行软件设计时应着重考虑 UE 以及 HCI 的软硬件环境及资源.

3.2 NB-IoT 加密方案

本节我们详述轻量级窄带物联网应用系统中高效可验证的加密方案,具体构建过程如下:

1) $CA\_Setup(\lambda,U)\rightarrow GP$

输入安全参数 λ 和通用属性集,利用 λ 生成阶为大素数 p 的群 G 和 G_T,将 G 的生成元 g 和 p 作为全局公共参数 GP. 定义一个双线性映射 $e:G\times G\rightarrow G_T$. 我们选取 2 个强抗碰撞的 Hash 函数 $H:\{0,1\}\rightarrow\mathbb{Z}_p$和 $H_1:G_T\rightarrow\{0,1\}^{\log p}$. 通过随机语言及将全局身份表示 GID 映射到 G 中的元素中.

2) $AA\_Setup(GP)\rightarrow(PK_k,SK_k)$

属性授权机构会针对每个授权机构 A_k 管理的每个属性 i,选择 2 个指数 $x_i,y_i\in\mathbb{Z}_p$,每个 A_k 将 $SK_k=\{x_i,y_i\}_{\forall i}$作为其私钥.

3) $KeyGen(SK_k,GP,S,GID)\rightarrow SK_U$

用户访问系统时向属性机构 A_k 申请私钥,每个授权机构 A_k 都会执行 AA_Setup 算法. 根据每个用户的唯一身份标识符 GID 以及每个属性 $i\in S$ 生

成相对应的密钥,计算 $SK_U=g^{\alpha_i}H(GID)^{y_i}$ 将私钥结果 SK_U 发送给用户.

4) $Offline.Enc(GP)\rightarrow IT$

这一阶段在数据属主终端设备上执行.但设备重新启动时,我们可以在离线阶段事先处理一些复杂计算,将结果即临时密文存储在移动终端设备上.具体算法为:假设本方案中最大属性集为 U,对于每个 $j\in[1,U]$,随机选一组 $\lambda_j',y_j',\alpha_j',\varphi_j',r_j'\in\mathbb{Z}_p$,计算 $\forall j:C_{1,j}=e(g,g)^{\lambda_j'}e(g,g)^{\alpha_j'r_j}$,$C_{2,j}=g^{r_j}$,$C_{3,j}=g^{y_j'r_j}g^{\varphi_j'}$.

5) $Online.Enc(IT,m,GP,PK_k,(\boldsymbol{M},\rho))\rightarrow(CT,Token)$

数据属主外派数据到服务器之前,需运行算法加密消息 m 成密文之后发送给云服务器.

① 数据属主随机选择 $ck\in G_T$,计算对称密钥 $sk=H'(ck)$,使用对称密钥 sk 加密数据 m,生成数据密文(data ciphertext, DC),另外计算验证令牌:$Token=H_1(H_0(DC)\parallel CT')$.

② 数据属主加密对称密钥 ck.

(i) 输入 LSSS 访问结构 $(\boldsymbol{M},\rho)$,其中函数 ρ 与 $\boldsymbol{M}$ 的行和属性相关.

(ii) 随机选择 $s\in\mathbb{Z}_p$ 作为加密指数.首先选择随机向量 $\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)\in\mathbb{Z}_p$,向量 $\boldsymbol{W}\in\mathbb{Z}_p^n$,其第 1 个元素为 0.

首先计算 $\forall j\in[1,l]:\lambda_j=\boldsymbol{M}_j\boldsymbol{v}$($\boldsymbol{M}_j$ 为访问矩阵 $\boldsymbol{M}$ 的第 j 行向量)和 $\varphi_j=\boldsymbol{M}_j\boldsymbol{W}$.而后计算密文 $C_0=e(g,g)^sck$,$C_{4,j}=\lambda_j-\lambda_j'$,$C_{5,j}=(\alpha_j-\alpha_j')r_j$,$C_{6,j}=(y_j-y_j')r_j$,$C_{7,j}=\varphi_j-\varphi_j'$.

最终密文为 $CT=\{(\boldsymbol{M},\rho),DC,C_0,\{C_{1,j},C_{2,j},C_{3,j},C_{4,j},C_{5,j},C_{6,j},C_{7,j}\}_{\forall j\in[1,l]}\}$.

6) $GenToken(SK_U,GP,S)\rightarrow(TK_U,Key)$

用户在重启移动设备时,选择随机数 $Z\in\mathbb{Z}_p$ 生成一个相关的转换密钥 $TK_U=(SK_U^{1/Z},H(GID)^{1/Z})$.

7) $Out.Decrypt(GID,GP,CT,TK_U)\rightarrow CT'$

用户将基于访问策略 $(\boldsymbol{M},\rho)$ 的密文 CT 和转换密钥交给云代理服务器进行部分密文解密.

进行计算:

$$C_{1,j}'=C_{1,j}e(g,g)^{C_{4,j}}e(g,g)^{C_{5,j}},$$

$$C_{2,j}'=e(H(GID),C_{3,j}g^{C_{6,j}}g^{C_{7,j}}),$$

$$C_3'=e(g^{\alpha_j/Z}H(GID)^{y_j/Z},C_{2,j}).$$

若用户属性满足访问策略 $(\boldsymbol{M},\rho)$,则找出 1 组随机值 $C_1,C_2,\cdots,C_n\in\mathbb{Z}_p$ 满足:$\sum_{j\in U}C_j\boldsymbol{M}_j=(1,0,0,\cdots,0)$,并计算 $CT_1=\prod_{j\in U}C_{1,j}'^{C_j}C_{2,j}'^{C_j}$,$CT_2=\prod_{j\in U}C_3'^{C_j}$.

将结果 $CT'=\{CT_1,CT_2\}$ 作为部分解密 CT' 返回给终端用户.

8) $Decrypt(CT',GP,Key)\rightarrow m$

用户收到云代理服务器发送的部分解密密文 CT' 后,执行该算法进行解密数据.计算对称密钥 $ck=C_0CT_2^z/CT_1$.最后,通过进一步计算,验证等式 $Token=H_1(H_0(DC)\parallel CT')$ 是否成立.

若等式成立,则云解密正确,而后使用 ck 解密密文 CT',最终获得明文 m;若等式不成立则返回 $\perp$.

4 实验结果与分析

4.1 NB-IoT 实验环境

本文选取资源受限的 NB-IoT 终端 UE 作为数据属主,UE 的主控芯片采用基于 ARM Cortex-M0+内核的 32 位微控制器.UE 的硬件实物为智能燃气表,如图 3 所示:

Fig. 3 UE hardware physical map

图 3 UE 硬件实物图

另外,我们选取 64 位操作系统 Windows10 的 PC(时钟频率为 3.20 GHz)作为 NB-IoT 人机交互客户端 HCI,将其作为数据访问用户.在我们的 NB-IoT 智能燃气表应用系统中,终端 UE 将采集到的数据加密后发送到华为云服务器,而后人机交互客户端 HCI 从云服务器上获取相应密文,并解密获得数据信息,完成一次数据的通信传输.

为了验证 OO-MA-CP-ABE 方案的可行性,并评估其实际性能.本节利用 0.5.14 版本的 Paring-based cryptography library[16] 对 OO-MA-CP-ABE 方案进行实验.我们将对访问结构为 LSSS 的 HW[12],GHW[13],LW[15] 方案和本文方案就在线加密和用户解密阶段进行实验.上述 2 个对比实验有关时间的统计是在本文选取的人机交互客户端

HCI 上执行的,主要配置前文已述. 另外,我们在 ARM 架构下的 NB-IoT 终端 UE 上执行的加密方案耗时大约 120 ms,而在 HCI 端执行加密只需 8 ms 左右,解密数据耗时 1.8 ms 左右. 一次完整的数据传输完成需要 15 s 左右(极限情况下需要 30 s 左右). 需要指出的是,所有对比实验的结果都是取运行 30 次后所得的平均值.

图 4 给出了 HW[12],GHW[13],LW[15]方案与本文 OO-MA-CP-ABE 方案在不同属性个数不同的情况下,各个方案在在线加密阶段所需的时间对比. 在实验过程中,假设属性个数由 2 变化到 20. 如图 4 所示,我们的 OO-MA-CP-ABE 方案在在线加密阶段计算开销与属性数目无关,几乎保持恒定,可以应用于计算能力弱且资源受限的移动终端用户. 虽然本方案耗时略高于 HW[12]方案,但用户解密阶段耗时远远低于 HW[12]方案,因此本文方案整体更优.

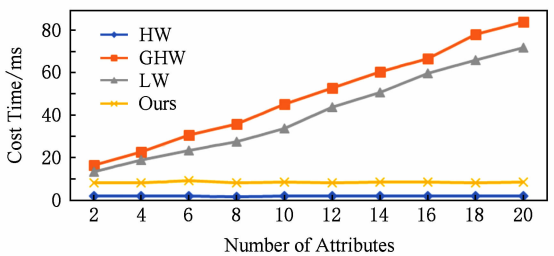

Fig. 4 Comparison of encryption time

图 4 在线加密开销时间比较

图 5 给出了 HW[12],GHW[13],LW[15]方案与本文 OO-MA-CP-ABE 方案在不同属性个数不同的情况下,各个方案用户解密阶段所需的时间对比. 在实验过程中,假设属性个数由 2 变化到 20. 如图 5 所示:

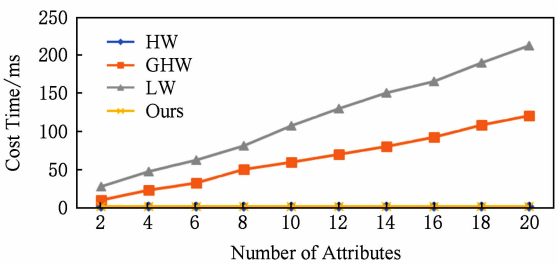

Fig. 5 Comparison of final decryption time

图 5 用户解密开销时间比较

我们的 OO-MA-CP-ABE 方案在用户解密阶段计算开销与属性数目无关,几乎保持恒定,我们将大量复杂的运算外包给云服务器,解密时间远远少于 HW[12]和 LW[15]方案. 虽然本方案耗时与 GHW[13]方案相近,但在线加密阶段耗时远远低于 GHW[13]方案,因此本文方案整体更优,更适合于计算能力弱且资源受限的移动终端用户.

4.2 正确性分析

本文构造的 OO-MA-CP-ABE 方案的正确性主要依赖于双线性映射的性质. 我们通过公式来证明本方案的正确性.

我们在方案构造中定义用户属性集合 S,以及与用户属性集合 S 相关的转换密钥 TK_U. 与此同时,我们定义一个访问策略$(\boldsymbol{M},\rho)$,以及和访问策略$(\boldsymbol{M},\rho)$相关的密文 CT. 我们在方案构造中计算获得:

$$C'_{1,j}=C_{1,j}e(g,g)^{C_{4,j}}e(g,g)^{C_{5,j}}=$$
$$e(g,g)^{\lambda'_j}e(g,g)^{\alpha'_j r_j}e(g,g)^{(\lambda_j-\lambda'_j)}e(g,g)^{(\alpha_j-\alpha'_j)r_j}=$$
$$e(g,g)^{\lambda_j}e(g,g)^{\alpha_j r_j}.$$
$$C'_{2,j}=e(H(GID),C_{3,j}g^{C_{6,j}}g^{C_{7,j}})=$$
$$e(H(GID),g^{y'_j r_j}g^{\varphi'_j}g^{(y_j-y'_j)r_j}g^{\varphi_j-\varphi'_j})=$$
$$e(H(GID),g^{y'_j r_j}g^{\varphi_j}).$$
$$C'_3=e(g^{\alpha_j/Z}H(GID)^{y_j/Z},C_{2,j})=$$
$$e(g^{\alpha_j/Z},g^{r_j})e(H(GID)^{y_j/Z},g^{r_j})=$$
$$e(g,g)^{\alpha_j r_j/Z}e(H(GID),g)^{y_j r_j/Z}.$$

若转换密钥 TK_U 中拥有 GID 的用户属性集合 S 满足密文 CT 中的访问策略$(\boldsymbol{M},\rho)$要求,则可说明 OO-MA-CP-ABE 方案的正确性. 也就是说,$\sum_{j\in I}\lambda_j C_j=s$,$\sum_{j\in I}y_j C_j=0$,即可通过恢复密钥$\{Z\in\mathbb{Z}_p\}$,转换密钥 TK_U 和密文 CT 构建以下的公式验证本文方案的正确性. 具体验证步骤如下:

由本节可知:

$$CT_1=\prod_{j\in U}C'^{C_j}_{1,j}C'^{C_j}_{2,j}=\prod_{j\in U}e(g,g)^{\lambda_j C_j}e(g,g)^{\alpha_j r_j C_j}\times$$
$$e(H(GID),g)^{y_j r_j C_j}=\prod_{j\in U}e(g,g)^{\lambda_j C_j}e(g,g)^{\alpha_j r_j C_j}\times$$
$$e(H(GID),g)^{y_j r_j C_j}e(H(GID),g)^{\varphi_j C_j}=$$
$$e(g,g)^{s}e(g,g)^{\sum_{j\in I}\alpha_j\lambda_j C_j}e(H(GID),g)^{\sum_{j\in I}y_j r_j C_j}.$$
$$CT_2=\prod_{j\in U}C'^{C_j}_3=$$
$$\prod_{j\in U}e(g,g)^{\alpha_j r_j C_j/Z}e(H(GID),g)^{y_j r_j C_j/Z}.$$

因此,我们可以进一步获得

$$\frac{CT_2{}^Z}{CT_1}=\left(\frac{\prod_{j\in U}e(g,g)^{\alpha_j r_j C_j/Z}e(H(GID),g)^{y_j r_j C_j/Z}}{e(g,g)^{s}e(g,g)^{\sum_{j\in I}\alpha_j\lambda_j C_j}e(H(GID),g)^{\sum_{j\in I}y_j r_j C_j}}\right)^Z=\frac{1}{e(g,g)^s}.$$

又因为 $C_0=me(g,g)^s$,所以解密用户可以通过计算 $C_0\dfrac{CT_2{}^Z}{CT_1}=me(g,g)^s\dfrac{1}{e(g,g)^s}=m$ 来恢复明文

消息 m. 至此,我们可以得出本文方案是正确的.

最终正确获得明文消息.

4.3 安全性分析

定义 2. 本文基于离散对数困难问题下利用 GID 解决了抵抗多个属性授权机构的合谋攻击和不同用户直接攻击. 本文方案基于具有 CPA 安全的 Waters 方案发展而来,因此也是 CPA 安全的. 在 l-BDHI 困难问题假设成立的情况下,任何多项式时间内敌手 A 不具备攻破本文方案的优势[17].

证明. 假设本文方案,存在被一个 PPT 敌手 A 以不可忽略的优势攻破的可能. 即构造模拟者 D,证明其可通过 A 以 $\varepsilon/2$ 的概率判定出 2 个 l-BDHI 随机元组 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l},e(g,g)^{1/\alpha})$ 和 $(\alpha\in\mathbb{Z}_p, T\in G_T)$.

执行 CA_Setup 算法,产生公共参数 GP,然后将 GP 交给敌手. 挑战者 C 会通过执行 AA_Setup 算法生成相应的主公私钥对 (PK_k,SK_k) 并发送给模拟者 D. 挑战者 C 选择 1 个随机值 $n\in\{0,1\}$,该值隐瞒敌手 A 和模拟者 D. $n=0$,将 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l},T)$ 设为元组,否则 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l},e(g,g)^{1/\alpha})$ 为元组. 模拟以下游戏:

初始化:敌手 A 指定将要被挑战的访问结构 $(\boldsymbol{M},\rho)^*$ 给 S.

建立:定义 Hash 函数 $H:\{0,1\}\to\mathbb{Z}_p$. I 代表本文模型中的所有属性授权机构集合. 模拟者 D 生成相关公共参数 GP,并生成属性授权机构公钥集 PK_k 一起发送给敌手 A. 敌手 A 将密文提交给预言机解密,如果成功则返回明文 m 给敌手.

阶段 1:敌手 A 选择一组用户 GID 和用户属性集合 S. 基于 $I-I'$ 中的非假冒授权机构,向模拟者 D 多次提交 (S,GID) 进行密钥询问. 注意:S 中的每一个属性都不满足访问结构 $(\boldsymbol{M},\rho)^*$,并且来自于可靠的属性授权机构. 执行 $KeyGen$ 算法,产生用户私钥 SK_U 发送给敌手 A.

挑战:敌手 A 制定 2 个等长明文消息 M_0,M_1 给挑战者 C;模拟者 D 选择 1 个随机值 $b\in\{0,1\}$,执行加密算法产生挑战密文 CT,最后将 CT 发送给敌手 A. 如果 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l},T)\in(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l}e(g,g)^{1/\alpha})$,则 D 模拟成功.

阶段 2:重复阶段 1 的操作.

猜想:敌手 A 输出 b 的猜测值 $b'\in\{0,1\}$. $\exists b=b'$ 则敌手 A 获胜.

这里定义敌手 A 的优势为 $Adv(D)=Pr[b=b']-1/2$,其成功概率为 $Pr[b=b']$.

当 $n=0$,D 猜对 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l},T)$ 为元组成功的概率为 1/2;

当 $n=1$,D 猜对 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^l},e(g,g)^{1/\alpha})$ 为元组成功的概率为 $1/2+\varepsilon$;

所以综上所述:D 模拟游戏成功的概率为

$$Adv(D)=\frac{1}{2}\left(\frac{1}{2}+\varepsilon+\frac{1}{2}\right)-\frac{1}{2}=\frac{\varepsilon}{2}.$$

该结果是可以忽略不计的,即是 l-BDHI 困难的. 因此任意敌手 A 在上述攻击游戏中,在多项式时间内能获胜的概率是可忽略的,本方案是选择明文攻击(CPA)安全的. 证毕.

4.4 性能分析

本节对本文方案性能作了简单分析.

首先在加密阶段,我们进行分步处理:离线阶段和在线阶段. 在离线加密阶段,我们将大量的复杂运算,如双线性配对和幂乘计算提前进行处理,将结果存储在设备上. 设备将在充电状态下或者空闲状态时自动离线完成;在线阶段时,只需付出极小的代价进行简单计算,就可快速完成加密. 极大降低了终端计算开销,节省低功耗终端设备的大量电量消耗. 解密阶段时,我们也将大量复杂计算外包在云服务器上,减少了数据用户端的解密运算开销,并且大大提高了解密效率. 与此同时,我们还融入了隐藏访问结构方案和验证外包解密正确性的算法,进一步保证了本文的可靠性和安全性[18]. 本节给出了 OO-MA-CP-ABE 方案与已有的相关方案在功能性、计算开销和通信开销方面的对比分析.

表 1 给出了本文方案和其他方案的特征功能比较,主要包括是否支持多个属性授权机构、访问策略的表现形式、是否支持外包计算可验证性、是否支持在线/离线加密和外包解密. 由表 1 可知:BSW[9],GHW[13],HW[12] 方案是一般单授权中心机制,随着用户属性的增加,授权机构的负担与风险将加大. 本文和 LW[15] 等方案采用多属性授权机构,更符合分布式应用需求,更为高效灵活,还可以抵抗合谋攻击. 但是 MDD[11] 和 LW[15] 方案既不能支持外包加密也不能支持外包解密,用户计算开销过大,不适合实际应用于轻量级窄带物联网应用系统. 此外,上述方案均没有验证外包计算的正确性. 因此,本文方案优于现有方案,具有更强的可扩展性.

表 2 给出计算性能和密文长度的比较. 在详细分析本文的计算开销和通信开销之前,我们先定义后文所使用的相关符号,设 E 表示在群 G 和 G_T 的

1 次指数操作花销,P 表示 1 次双线性配对操作运算花销,l 代表 LSSS 访问结构属性的行数或者访问树中间节点数,$|G|$,$|G_T|$,$|\mathbb{Z}_p|$ 分别表示 G,G_T,$\mathbb{Z}_p$ 的长度,U 表示解密时的系统属性个数,S 为在群 G 和 G_T 的 1 次点乘操作花销. 文中的计算开销主要源于双线性运算和幂乘运算. 在表 2 中,我们列出了终端用户的在线加密开销和解密开销以及相应的密文长度. 相比于 BSW[9],GHW[13],HW[12],LW[15] 方案,本文方案在加密阶段,用户端只需要做简单点乘运算,大大减少了幂乘运算开销. 另外,本文还将大量的线性配对和幂乘计算开销外包至云服务器,用户只需一次幂乘计算,大大降低了终端解密用户的计算负担. 虽然本文的密文长度相较于 GHW[13],HW[12] 方案略微较长,但是其加解密负担较低,效率高的同时还加入了验证外包解密正确性的算法,安全性可靠性得到了保障.

Table 1 Comparison of Features and Functions of this Program and Other Programs

表 1 本文方案和其他方案的特征功能比较

Schemes	ABE-Type	Access	Offline. Encryption	Out. Decryption	Verification	Multi-Authority
BSW[9]	CP-ABE	Threshold	√	×	×	×
HW[12]	CP-ABE	LSSS	√	×	×	×
GHW[13]	CP-ABE	LSSS	×	√	×	×
MDD[11]	CP-ABE	Access Tree	×	×	×	√
LW[15]	CP-ABE	LSSS	×	×	×	√
Ours	CP-ABE	LSSS	√	√	√	√

Note: √ means whether it supports this feature, × means whether this feature is not supported.

Table 2 Comparison of Calculation Performance and Ciphertext Length Between this and Other Schemes

表 2 本文方案和其他方案计算性能和密文长度的比较

Schemes	Online. Encryption	DU. Decryption	Length of Ciphertext
BSW[9]	$(U+1)E+S$	$2(UP+E+l)$	$2U\|G\|$
HW[12]	$lS+E$	$l(P+E+5S)$	$(3l+1)\|G\|+\|G_T\|+\|\mathbb{Z}_p\|$
GHW[13]	$2(l+1)E$	E	$(2l+1)\|G\|+\|G_T\|$
LW[15]	$(5l+1)E$	$(2P+E)U$	$2l\|G\|+(l+1)\|G_T\|$
Ours	$2lS+2E$	E	$(2l+1)\|G\|+(l+1)\|G_T\|+4l\|\mathbb{Z}_p\|$

Note: U represents the set of attributes required for decryption; E indicates the time for one exponentiation operation in the group G and G_T; $|G|$, $|G_T|$ and $|\mathbb{Z}_p|$ denote the length of each element in G, G_T and $\mathbb{Z}_p$; l represents the number of rows of the access structure matrix; P represents time required for a pairing operation; S indicates the time for a multiplication in the group G and G_T.

5 总 结

本文提出了一种新的轻量级 NB-IoT 应用系统中高效可验证的加密方案:在线/离线加密和外包解密的多机构 CP-ABE 加密方案 OO-MA-CP-ABE. 在多个属性授权机构的背景下,采用更灵活的访问控制策略,大大减轻了授权中心的负担和风险. 融入在线/离线加密和外包解密技术,将大量昂贵的计算外包给云服务器,最小化终端用户的计算开销和存储负担,很好地解决计算能力较弱且资源受限的 NB-IoT 云存储数据安全问题,提高了资源访问控制效率,此外,密钥存储在云端,降低访问过程中数据通信量. 最后,通过验证外包解密正确性的算法,进一步保证了本文的可靠性和安全性.

参 考 文 献

[1] Wang Y P E, Lin X, Adhikary A, et al. A primer on 3GPP narrowband Internet of things [J]. IEEE Communications Magazine, 2017, 55(3): 117-123

[2] Zayas A D, Merino P. The 3GPP NB-IoT system architecture for the Internet of things [C] //Proc of IEEE Int Conf on Communications Workshops. Piscataway, NJ: IEEE, 2017: 277-282

[3] Oh S M, Shin J S. An efficient small data transmission scheme in the 3GPP NB-IoT system [J]. IEEE Communications Letters, 2017, 21(3): 660-663

[4] Yu Changsheng, Yu Li, Hong Zhen, et al. Research on the security capacity of narrow-band Internet of things physical layer based on amplified forwarding and collaborative congestion [J]. Journal of Transduction Technology, 2017, 30(4): 575-581 (in Chinese)
(余昌盛, 俞立, 洪榛, 等. 基于放大转发和协作拥塞的窄带物联网物理层安全容量研究[J]. 传感技术学报, 2017, 30(4): 575-581)

[5] Sun Zhixin, Hong Hanshu. Some reflections on security issues in NB-IoT [J]. ZTE Technologies, 2017, 23(1): 47-50 (in Chinese)
(孙知信, 洪汉舒. NB-IoT 中安全问题的若干思考[J]. 中兴通讯技术, 2017, 23(1): 47-50)

[6] Shamir A. Identity-based cryptosystems and signature schemes [G] //Advances in Cryptology. Berlin: Springer, 1984: 47-53

[7] Sahai A, Waters B. Fuzzy Identity-based encryption [G] // LNCS 3494: Proc of EUROCRYPT'05. Berlin: Springer, 2005: 457-473

[8] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[9] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of IEEE Symp on Security and Privacy(SP'07). Piscataway, NJ: IEEE, 2007: 321-334

[10] Chase M. Multi-authority attribute based encryption [C] // Proc of the 4th Conf on Theory of Cryptography. Berlin: Springer, 2007: 515-534

[11] Ma Dandan, Chen Qin, Dang Zhengqin, et al. Ciphertext policy encryption mechanism based on multi-attributes organization [J]. Computer Engineering, 2012, 38(10): 114-116 (in Chinese)
(马丹丹, 陈勤, 党正芹, 等. 基于多属性机构的密文策略加密机制[J]. 计算机工程, 2012, 38(10): 114-116)

[12] Hohenberger S, Waters B. Online/offline attribute-based encryption [G] //LNCS 8383: Proc of Public-Key Cryptography. Berlin: Springer, 2014: 293-310

[13] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C] //Proc of the USENIX Security Symp. Berkeley, CA: USENIX Association, 2011: 3-23

[14] Zhou Kai, Ren Jian. Secure fine-grained access control of mobile user data through untrusted cloud [C] //Proc of the 23rd IEEE Int Conf on Computer Communication and Networks. Piscataway, NJ: IEEE, 2016: 49-54

[15] Lewko A, Waters B. Decentralizing attribute-based encryption [C] //Proc of Advances in Cryptology EUROCRYPT'11. Berlin: Springer, 2011: 568-588

[16] Cheng M. The pairing-based cryptography library [OL]. [2017-08-10]. https://crypto. stanford. edu/pbc/download. html

[17] Ma Haiying, Zeng Guojun, Wang Zhanjun, et al. Efficient and provably secure attribute-based online/offline encryption mechanism [J]. Journal on Communications, 2014, 35(7): 104-112 (in Chinese)
(马海英, 曾国荪, 王占君, 等. 高效可证明安全的基于属性的在线/离线加密机制[J]. 通信学报, 2014, 35(7): 104-112)

[18] Ruj S, Stojmenovic M, Nayak A. Privacy preserving access control with authentication for securing data in clouds [C] // Proc of the 12th IEEE/ACM Int Symp on Cluster, Cloud and Grid Computing. Piscataway, NJ: IEEE, 2012: 556-563

Qian Hanjia, born in 1994. Master. Her main research interests include embedded system, machine learning, wireless sensor network.

Wang Yihuai, born in 1962. PhD, professor. His main research interests include embedded system, machine learning, wireless sensor network.

Peng Tao, born in 1989. PhD. His main research interests include embedded system, machine learning, wireless sensor network.

Chen Cheng, born in 1994. Master. His main research interests include embedded system, machine learning, wireless sensor network.

Luo Xizhao, born in 1978. PhD, associate professor. His main research interests include cryptography, security of IoT, and computational complexity.