面向卫星物联网的无证书双边访问控制方案*

张华乐，陆　俊，林　航，颜　申
（国网安徽省电力有限公司信息通信分公司，安徽　合肥　230022）

摘　要：作为物联网设备互通的新范式，卫星物联网能够有效弥补传统地面物联网的不足。然而，卫星物联网环境下设备间交互的安全保障能力仍有待提高。鉴于此，提出了一种面向卫星物联网的无证书双边访问控制方案。本方案采用无证书公钥加密技术避免了传统加密方案中的密钥托管和证书管理问题，并基于匹配加密技术实现了发送端和接收端的双边访问控制。此外，通过将部分加解密工作外包给边缘服务器的方式，减轻了终端设备的计算负担。基于标准困难假设的安全分析证实了本方案的安全性，而性能分析则表明了本方案的实用性。

关键词：卫星物联网；无证书公钥加密；匹配加密；双边访问控制
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.01.004
引用格式：张华乐，陆俊，林航，等. 面向卫星物联网的无证书双边访问控制方案［J］. 网络安全与数据治理，2025，44(1)：21-29.

A certificateless bilateral access control scheme for satellite IoT

Zhang Huale，Lu Jun，Lin Hang，Yan Shen
(Information and Communication Branch，State grid Anhui Electric Power Co.，Ltd.，Hefei 230022，China)

Abstract：As a novel paradigm for the interconnection of Internet of Things (IoT) devices，satellite IoT effectively addresses the limitations inherent in terrestrial IoT networks. However，the security of device interactions within the satellite IoT environment remains an area ripe for enhancement. In view of this，this article proposes a certificateless bilateral access control scheme for satellite IoT. This scheme employs certificateless public key encryption technology to avoid the issues of key escrow and certificate management inherent in traditional encryption schemes，and achieves bilateral access control between the sender and receiver based on matching encryption technology. In addition，by outsourcing part of the encryption and decryption tasks to edge servers，the computational burden on terminal devices has been reduced. Security analysis based on standard hardness assumptions confirms the security of the scheme，while performance analysis demonstrates its practicality.

Key words：satellite Internet of Things；certificateless public key encryption；matching encryption；bilateral access control

0　引言

随着地轨卫星网络和高通量卫星等新型通信手段的出现，物联网正逐步迈向“地-天-空”一体化的模式。作为促进物联网设备间通信的下一代网络，相较传统地面物联网，融合卫星和物联网特征的卫星物联网（Satellite Internet of Things，SIoT），能够有效克服偏远地区网络覆盖能力不足的局限性，实现更大范围的实时、有效通信[1]。

由于终端设备计算和能源等资源的限制，如何实现物联网环境中信息交互的安全性和实用性成为一个亟待解决的问题。无证书公钥加密技术（Certificateless Public Key Cryptography，CL-PKC）的提出[2]，避免了传统公钥基础设施（Public Key Infrastructure，PKI）密码体制中的密钥托管和证书管理问题，在提供安全性保障的同时，有效减轻了终端设备的计算和存储负担，成为当前物联网领域研究的热点。例如，Kumari 等人[3]基于无证书公钥加密技术设计了一种适用于物联网的认证协议，实现了对物联网终端的安全认证。Deng 等人[4]针对电力物联网环境，提出了一种无证书公钥加密技术的安全认证和密钥交换协议，在对终端完成安全认证的基础上，通过协商的安全会话密钥实现了设备与服务商之间的安全通信。考虑到物联网中终端有限的计算资源，Cui 等人[5]设计了一种基于椭圆曲线的无证书公钥加密方案，该方案

*基金项目：国网安徽省电力有限公司科技项目（521207240003）

利用椭圆曲线的点乘运算代替复杂的双线性配对操作，有效减轻了终端在认证过程中的计算负担。然而，上述的方案均侧重于物联网环境中的单边安全性，即关注作为数据发送方的终端设备的安全性。

此外，也有部分方案采用信号加密和属性基加密等方式解决物联网中的安全交互问题。信号加密结合加密和签名技术，以公钥验签的方式实现了对数据发送方的真实性保障[6]，而基于属性的加密方案虽然能够实现对接收方的细粒度访问，但通常不支持对数据发送方的访问控制[7]。因此，需要一种能够在物联网环境中进行双边访问控制的方法，提升数据的安全保障和控制能力。

匹配加密（Matchmaking Encryption，ME）能够为发送方和接收方提供双边访问控制[8]。ME 允许发送方为接收方设定一个访问域，同时使接收方能验证密文是否源自合法的发送方。然而，在当前研究方案中[9-10]，加密、解密过程仍大多完全依赖于计算资源受限的终端设备，并不适用于作为下一代物联网范式的卫星物联网环境。鉴于此，本文提出了一种面向卫星物联网的无证书双边访问控制方案，主要贡献如下：

（1）基于无证书加密和匹配加密技术，在避免传统加密方案密钥托管和证书管理问题的基础上，实现了发送端和接收端的双边访问控制，确保只有满足条件的发送端和接收端才能进行有效的数据交互，提升了物联网环境中的数据安全保障和控制能力。

（2）不同于传统基于双线性配对的方案，本方案采用椭圆曲线加密技术减少终端的计算负担，并在此基础上将终端的部分加解密工作外包给边缘服务器，进一步减轻了终端设备的计算开销。

（3）基于标准困难假设的安全分析证明了本方案的安全性；而性能分析则表明，相较于现有方案，本方案中终端设备承担的计算开销更小，具有更高的实用性。

1　相关工作

本节对本方案所涉及的无证书公钥加密和双边访问控制进行回顾。

（1）无证书公钥加密。因其有效避免了传统 PKI 密码体制中的密钥托管和证书管理问题而受到广泛关注[11]。近年来，有部分学者基于无证书公钥加密和双线性配对技术进行物联网安全方案的构建[12-14]。例如，Ali 等人[12]基于无证书公钥加密提出了一种面向车联网的安全通信方案。

然而，双线性配对操作的复杂性导致了终端设备需要承担较大的计算开销。为应对这一问题，许多学者提出了不依赖双线性配对操作的无证书加密方案。近年来，Lu 等人[15]提出了一种适用于物联网环境的无证书可搜索公钥加密方案，该方案同时避免证书管理问题和双线性配对操作，减少了计算开销。Liu 等人[16]提出了一种面向工业物联网的无证书公钥认证加密方案，实现了轻量级计算。Elhabob 等人[17]针对云辅助的车联网环境，提出了一种无配对的无证书公钥加密方案，该方案实现了对云中存储数据的高效检索与访问。因此，构建轻量级的无证书加密方案，以适应计算能力受限的物联网环境，仍是当前的研究热点和挑战。

（2）双边访问控制。2021 年，Ateniese 等人[9]提出了一种基于匹配加密的双边访问控制方案，在该方案中，发送方和接收方能够指定对方必须满足的策略，并通过同时验证发送方和接收方的方式，提供了更强的访问控制。在此基础上，Francati 等人[18]提出了基于身份的匹配加密方案，该方案允许发送方和接收方基于双方的身份进行细粒度的访问控制。随后，Chen 等人[19]提出了基于标准假设的匹配加密方案，该方案在不依赖随机预言模型的情况下提供了真实性的安全保证。Wu 等人[20]提出了一种基于模糊身份的匹配加密方案，在发送方和接收方的属性有一定数量重叠的情况下，可以恢复加密的消息。

然而，在上述方案中，密钥完全由第三方可信实体密钥生成中心负责生成，导致了密钥托管的问题。为应对这一问题，Chen 等人[10]提出了适用于物联网的无证书匹配加密方案，并构建了两种具体的方案。第一种基于双线性配对进行无证书匹配加密方案的构建，第二种则是无配对操作的轻量级匹配加密方案。Yang 等人[21]设计了一种轻量级的无证书匹配加密方案，有效减少了计算负担。然而，上述方案中的加解密过程仍依赖于计算资源受限的终端设备，需要探索更为适用的方案进一步减轻终端设备的计算压力。因此，本方案采取将终端的部分加解密工作外包给边缘服务器的方式，减轻终端设备的计算开销。

2　预备知识

本节给出了方案涉及的密码学知识及困难假设。

2.1　符号及含义

表 1 展示了方案中涉及的符号及其含义。

2.2　椭圆曲线密码学

椭圆曲线密码学（Elliptic Curve Cryptography，ECC）基于椭圆曲线离散对数困难问题，主要优势在于其较短的密钥长度、快速的加解密速度、高安全性能、较低的实现成本以及较小的存储需求。与其他的公钥加密方式相比，ECC 更加适用于一些计算资源和存储空间受限的环境[22]。其定义如下：

表 1　符号及含义

符号	描述
G	循环群组
q	群 G 的素数阶
P	群 G 的生成元
h_0，h_1，h_2	哈希函数
l，n	字符串的长度参数
φ	多项式时间可计算填充函数
a	发送端的身份
b	接收端的身份
snd	发送端中的目标身份
rcv	接收端中的目标身份
msk	系统主密钥
mpk	系统主公钥
ek_a	发送端 a 的加密密钥
pk_a	发送端 a 的公钥
dk_b	接收端 b 的解密密钥
pk_b	接收端 b 的公钥
m	明文信息
C_0，C_1，C_2	部分密文
C	密文
D_1	部分解密结果
$\oplus$	XOR 操作

在有限域内，存在一个被定义为 $y^2 = x^3 + cx + d \pmod p$ 的椭圆曲线 e，其中 c 和 d 是有限域中的元素，且满足 $4c^3 + 27d^2 \neq 0$。标量乘法运算是椭圆曲线密码学中的关键运算。对于椭圆曲线上任取一点 P 有 $nP = P + P + \cdots + P$（n 次），其结果仍是椭圆曲线上的一点，其中 $n \in Z_q^*$。

2.3　困难假设

（1）椭圆曲线离散对数问题

给定椭圆曲线 e 上阶为 q 的一点 P，G 为 P 生成的素数阶群。对于任意的 $Q \in G$，求解整数 $k \in Z_q^*$ 使得 P、Q 满足 $Q = kP$，如果没有任何概率多项式时间对手以一个不可忽略的优势通过 P 和 Q 计算获得 k，那么解决椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）是困难的[23]。

（2）计算性 Diffie-Hellman 假设

给定阶为 q 的循环群 G，P 为群 G 的生成元。对于任意的 x，$y \in Z_q^*$，给定 $Q = xP$，$R = yP$ 为 G 中两个随机元素，如果没有任何概率多项式时间对手以一个不可忽略的优势通过 P、Q 和 R 计算 xyP，那么解决计算性 Diffie-Hellman 假设（Computational Diffie-Hellman Assumption，CDH Assumption）是困难的[24]。

3　系统模型与安全模型

本节给出了系统模型、安全模型和方案的形式化定义。

3.1　系统模型

系统模型如图 1 所示，包含密钥生成中心、边缘服务器和终端三类实体和卫星网络。具体描述如下：

（1）密钥生成中心：作为可信的第三方实体，负责系统公共参数的生成，并为通信的发送端和接收端生成部分密钥。

（2）终端：根据其承担消息的发送或接收功能进一步分为发送端和接收端。发送端将密文通过卫星网络发送给接收端，但接收端成功解密密文需要同时满足以下条件：接收端的身份符合发送方的策略要求，同时发送方的身份也满足接收方的策略标准。

（3）边缘服务器：部署在终端附近的地面站中，有一定的计算资源，在本方案中分担了终端部分的加密和解密操作，以减轻终端的计算压力。

（4）卫星网络：为发送端和接收端的信息传输提供了安全的通信信道。

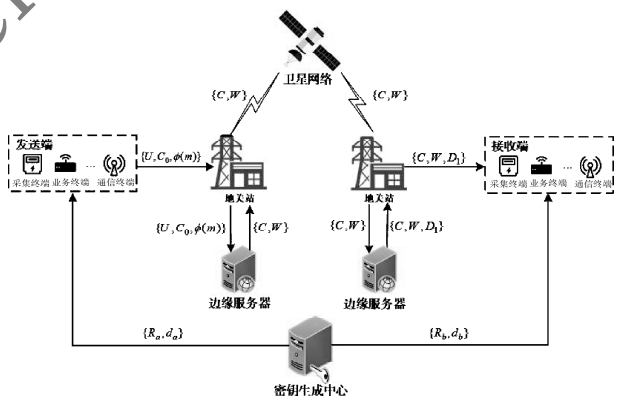

图 1　系统模型

3.2　安全模型

与文献［25－26］类似，本方案存在两种类型的敌手：类型Ⅰ为敌手 A_1 不知道系统的主密钥，但它可以选择一个随机数来代替任何一个终端的公钥；类型Ⅱ为敌手 A_2 可以获得系统的主密钥，但不能替换终端的公钥。此外，敌手 A_1 和 A_2 可以自适应地进行查询，且挑战者 B 输出对应的结果。敌手 A_1 和 A_2 可进行的查询如下：

加密密钥查询：在收到对 a_i 的查询后，B 返回发送端的密钥。

解密密钥查询：在收到对 b_i 的查询后，B 返回接收端的密钥。

替换公钥查询：A_1 可以替换发送端和接收端的公钥。

挑战者 B 和敌手 $A \in \{A_1, A_2\}$ 的博弈游戏定义如下：

初始化：输入安全参数，B 运行初始化算法，生成主公钥 mpk 和主密钥 msk。若 $A = A_1$，B 将 mpk 发送给 A；若 $A = A_2$，B 将 $\{\text{msk}, \text{mpk}\}$ 发送给 A。

阶段 1：若 $A = A_1$，A 可以进行加密密钥查询，解密密钥查询，替换公钥查询；若 $A = A_2$，A 可以进行加密密钥查询，解密密钥查询。

伪造：首先，A 将密文 $\{C, b, \text{snd}\}$ 发送给 B。其次，B 通过执行解密密钥生成算法和解密算法来生成 $\{\text{dk}_b, P_b\}$ 和明文 m。如果存在一个元组 $\{a, b, m\}$ 使得 $a = \text{snd}$，b 在上述阶段未被查询过且 $m \neq \perp$，则 B 返回 1；否则，B 返回 0。

如果对于任何多项式时间敌手 A，B 在上述游戏中输出 1 的优势可以忽略不计，则说明该方案具有安全性。

3.3 形式化定义

基于系统和安全模型，给出本方案的形式化定义：

（1）初始化：该算法输入安全系数 λ，输出系统的主公钥 mpk 和主密钥 msk。

（2）加密密钥生成：该算法输入主密钥 msk 和发送端的身份 a，并输出加密私钥 ek_a 和公钥 pk_a。

（3）解密密钥生成：该算法将主密钥 msk 和接收端的身份 b 作为输入，并输出解密私钥 dk_b 和公钥 pk_b。

（4）加密：包含发送端加密和外包加密两个部分。发送端以主公钥 mpk、加密私钥 ek_a、接收端 rcv 的部分公钥 P_{rcv} 和消息 m 作为输入，输出部分密文 C_0 和 $\varphi(m)$；外包加密将接收端的身份 rcv、公钥 pk_{rcv} 和 $\varphi(m)$ 作为输入，输出密文 C。

（5）解密：包含外包解密和接收端解密两个部分。外包解密将主公钥 mpk、发送端的身份 snd 和公钥 pk_a 作为输入，输出部分解密结果 D_1。接收端解密以解密私钥 dk_b、发送端的身份 snd，相应的公钥 P_{snd}、密文 C 和部分解密结果 D_1 作为输入，当且仅当发送端 snd 生成的密文 C 与接收端 b 相匹配时，输出消息 m，否则输出 $\perp$。

4 方案构建

本方案的构建主要包括初始化、加密密钥生成、解密密钥生成、加密、解密五个阶段。

4.1 初始化

初始化阶段由密钥生成中心执行，具体过程如下：

（1）选择一个阶为 q、生成元为 P 的群 G，和三个哈希函数：$h_0: \{0,1\}^* \times G \rightarrow Z_q^*$，$h_1: \{0,1\}^* \times G \times G \times G \rightarrow Z_q^*$ 和 $h_2: G \rightarrow \{0,1\}^l$。

（2）选择一个多项式时间可计算的填充函数 $\varphi: \{0,1\}^n \rightarrow \{0,1\}^l$，满足对于所有的 $m \in \{0,1\}^n$，在多项式时间内被正确填充，且 $\varphi(m)$ 是有效可逆的。

（3）输入安全系数 1^λ 后，随机选择 $s \in Z_q^*$，并计算 $P_0 = sP$。最后，得到主公钥 $\text{mpk} = \{G, q, P, P_0, h_1, h_2, \varphi\}$ 和主密钥 $\text{msk} = s$。

4.2 加密密钥生成

该阶段由密钥生成中心和发送端 a 共同执行，具体过程如图 2 所示，包括如下操作：

（1）密钥生成中心为发送端 a 随机选择 $r_a \in Z_q^*$，计算部分密钥 $R_a = r_a \cdot P$ 和 $d_a = r_a + s \cdot h_0(a, R_a)$，并将 $\{R_a, d_a\}$ 通过安全信道传输至发送端。

（2）发送端 a 验证等式 $d_a \cdot P = R_a + h_0(a, R_a) \cdot P_0$ 是否成立，以确保密钥生成中心部分密钥的正确性。

（3）若（2）成立，发送端 a 随机选择秘密值 $x_a \in Z_q^*$，并计算 $P_a = x_a \cdot P$。之后，以 $\text{pk}_a = (P_a, R_a)$ 和 $\text{ek}_a = (d_a, x_a)$ 分别作为其公钥和私钥。

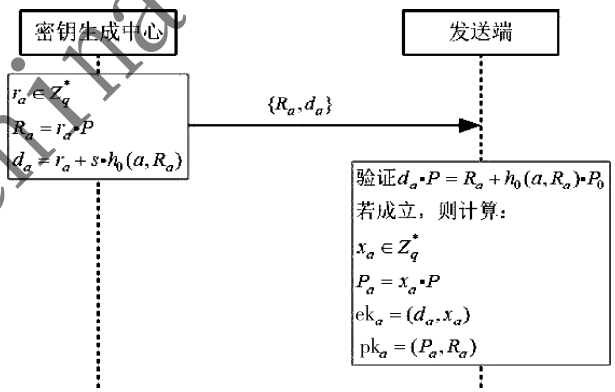

图 2　加密密钥生成阶段

4.3 解密密钥生成

解密密钥生成阶段由密钥生成中心和接收端 b 共同执行，如图 3 所示，具体过程如下：

（1）密钥生成中心为接收端 b 随机选择 $r_b \in Z_q^*$，计算部分密钥 $R_b = r_b \cdot P$ 和 $d_b = r_b + s \cdot h_0$（b，R_b），并将 $\{R_b, d_b\}$ 通过安全信道传输至接收端。

（2）接收端 b 验证等式 $d_b \cdot P = R_b + h_0(b, R_b) \cdot P_0$ 是否成立，以确保密钥生成中心部分密钥的正确性。

（3）若（2）成立，接收端 b 随机选择秘密值 $x_b \in Z_q^*$ 并计算 $P_b = x_b \cdot P$。最后，接收端根据密钥生成中心的部分密钥和其密值获得解密私钥 $\text{dk}_b = (d_b, x_b)$ 以及其公钥 $\text{pk}_b = (P_b, R_b)$。

4.4 加密

加密阶段对消息 $m \in \{0,1\}^n$ 进行加密，并选定目标接收端 $\text{rcv} = b$ 发送密文。该阶段共分为两部分：发送端

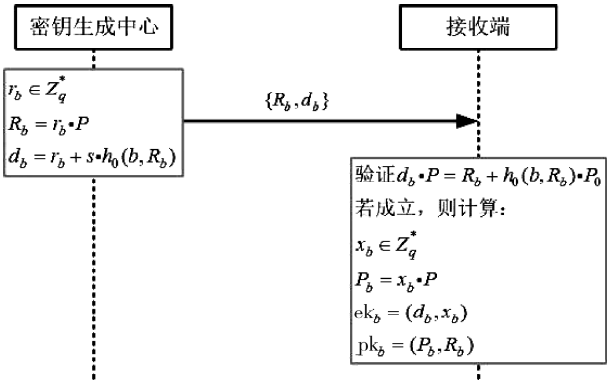

图 3　解密密钥生成阶段

加密和外包加密。发送端加密部分由发送端执行，具体操作如下：

（1）随机选择 $u \in Z_q^*$，并计算 $U = u \cdot P$。

（2）计算 $C_0 = (d_a + x_a) \cdot P_b$ 和 $\varphi(m)$ 并将 $\{U, C_0, \varphi(m)\}$ 传输给边缘服务器。

外包加密部分由边缘服务器完成，具体操作如下：

（1）计算 $C_1 = R_b + P_0 \cdot h_0(b, R_b)$ 和 $C_2 = P_b \cdot h_1(a, P_0, P_a, R_a)$。

（2）随机选择 $w \in Z_q^*$，并计算 $W = w \cdot P$。

（3）计算 $K_S = C_0 + U \cdot w \cdot C_2$ 和 $K_R = U \cdot w \cdot C_1$。

（4）计算 $V = \varphi(m) \oplus h_2(K_R) \oplus h_2(K_S)$。

（5）返回密文 $C = (U, V)$，并将 $\{C, W\}$ 通过卫星网络传输至接收端的边缘服务器。

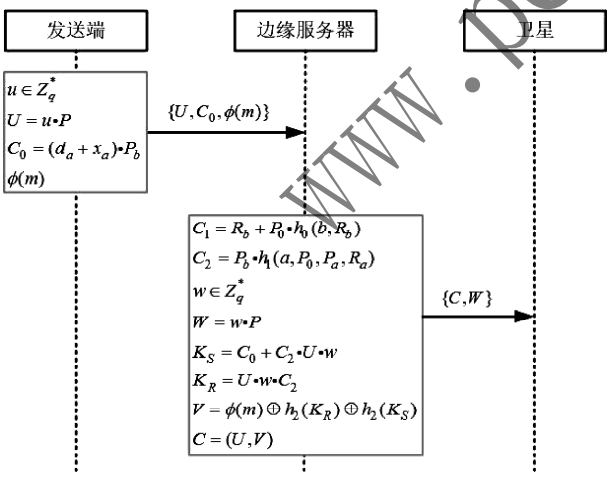

图 4　加密阶段

4.5　解密

解密阶段对发送端 snd = a 传输的密文进行解密。该阶段共分为两个部分：外包解密和接收端解密。

外包解密部分由边缘服务器完成，具体操作如下：

（1）计算 $D_1 = R_a + P_0 h_0(a, R_a) + P_a + h_1(a, P_0, P_a, R_a) \cdot U \cdot W$。

（2）将部分解密结果 D_1、密文 C 和 W 传输至接收端。

接收端解密部分由接收端执行，具体操作如下：

（1）接收端由获得的密文 $C = \{U, V\}$ 计算获得 $K'_R = U \cdot W \cdot d_b$ 和 $K'_S = x_b \cdot D_1$。

（2）进一步计算 $\varphi(m) = V \oplus h_2(K'_R) \oplus h_2(K'_S)$，若 $\varphi(m)$ 有效，则返回 m；否则，返回 $\perp$。

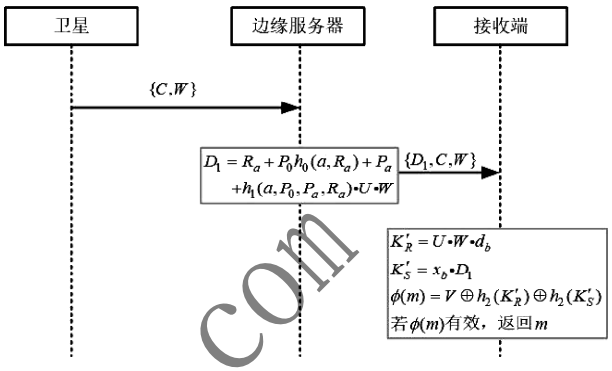

图 5　解密阶段

5　安全分析

本节将对方案的正确性及其安全性展开分析。

5.1　正确性分析

部分密钥正确性。当发送端获得密钥生成中心生成的部分密钥 $\{R_a, d_a\}$ 时，可通过式（1）对其进行验证。若验证等式 $d_a \cdot P = R_a + h_0(a, R_a) \cdot P_0$ 成立，则说明部分密钥合法。接收端对部分密钥的验证思路与发送端相同，可通过式（2）验证部分密钥的正确性。

$$\begin{aligned} d_a \cdot P &= [r_a + s \cdot h_0(a, R_a)] P \\ &= R_a + h_0(a, R_a) \cdot P_0 \end{aligned} \tag{1}$$

$$\begin{aligned} d_b \cdot P &= [r_b + s \cdot h_0(b, R_b)] P \\ &= R_b + h_0(b, R_b) \cdot P_0 \end{aligned} \tag{2}$$

解密正确性。当且仅当 a = snd 及 b = rcv 时，接收端才能成功解密获得信息 m。$\{K_R, K_S\}$ 为加密阶段计算所得，$\{K'_R, K'_S\}$ 为解密阶段计算所得，若 a = snd 及 b = rcv，则有：

$$\begin{aligned} K_R &= U \cdot w \cdot [R_b + P_0 h_0(b, R_b)] \\ &= U \cdot w \cdot P[r_b + s h_0(b, R_b)] \\ &= U \cdot W \cdot d_b = K'_R \end{aligned} \tag{3}$$

$$\begin{aligned} K_S &= C_0 + C_2 \cdot U \cdot w \\ &= (d_a + x_a) \cdot P_b + P_b \cdot h_1(a, P_0, P_a, R_a) \cdot U \cdot w \\ &= x_b[(d_a + x_a) \cdot P + h_1(a, P_0, P_a, R_a) \cdot U \cdot w \cdot P] \\ &= x_b \cdot D_1 = K'_S \end{aligned} \tag{4}$$

因此，$\varphi(m) = V \oplus h_2(K'_R) \oplus h_2(K'_S)$ 的计算是有效的，由 $\varphi(m)$ 获得的明文信息 m 是有效的。

5.2 安全性分析

定理 1：如果 CDH 困难性假设成立，则不存在多项式时间敌手能以不可忽视的优势攻破本方案，那么证明本方案是安全的。定理 1 可由引理 1 和引理 2 推断出。

引理 1：假设敌手 A_1 以不可忽略的优势 ε 攻破本方案，那么一个构建的算法 B 则可以优势 ε' 打破 CDH 困难性问题。

证明：给定一个元组 $\{P, yP, zP\}$，B 通过和 A_1 之间的交互计算得到 $D = yzP$。

初始化：B 设置 $P_0 = yP$，并将公共参数 $\{G, q, P, P_0, h_1, h_2, \varphi\}$ 发送给 A_1。

阶段 1：A_1 自适应地进行以下查询。

h_0 查询：B 维护一个哈希列表 $L_0 = \{id_i, R_i, \alpha_i\}$，其中 $id_i = a_i$ 或 b_i。如果之前查询过 id_i，则 B 返回 α_i，否则，B 随机选择 $\alpha_i \in Z_q^*$，返回 α_i，并将 $\{id_i, R_i, \alpha_i\}$ 添加到 L_0 中。

h_1 查询：B 维护一个哈希列表 $L_1 = \{a_i, P_0, P_a, R_a, \beta_i\}$，如果之前查询过 a_i，则 B 返回 β_i。否则，B 随机选择 $\beta_i \in Z_q^*$，返回 β_i，并将 $\{a_i, P_0, P_a, R_a, \beta_i\}$ 添加到 L_1 中。

h_2 查询：B 维护一个哈希列表 $L_2 = \{X_i, h_{2,i}\}$。如果之前已经查询过 X_i，则 B 返回 $h_{2,i}$。否则，B 随机选择 $h_{2,i} \in \{0, 1\}^n$，返回 $h_{2,i}$，并将添加到 L_2 中。

加密密钥查询：B 维护一个哈希列表 $L_3 = \{a_i, P_i, R_i, d_i, x_i\}$，如果之前查询过 a_i，B 返回 $\{P_i, R_i, d_i, x_i\}$。否则，B 随机选择 x_i，d_i，$\alpha_i \in Z_q^*$，计算 $P_i = x_i \cdot P$，$R_i = d_i P(\alpha_i P_0) - 1$，并设定 $h_0(a_i, R_i) = \alpha_i$，B 将 $\{a_i, R_i, \alpha_i\}$ 和 $\{a_i, P_i, R_i, d_i, x_i\}$ 分别添加到 L_0 和 L_3 中，返回 $\{P_i, R_i, d_i, x_i\}$。

解密密钥查询：B 维护一个哈希列表 $L_4 = \{b_i, P_i, R_i, d_i, x_i, r_i, c_i\}$。如果 b_i 已经被查询过，B 返回 $\{P_i, R_i, d_i, x_i\}$；否则，B 生成 $c_i \in \{0, 1\}$ 使得 $\Pr[c_i = 0] = \delta$。

(1) 如果 $c_i = 1$，B 随机选择 x_i，$r_i \in Z_q^*$，计算 $P_i = x_i P$，$R_i = r_i P$，将 $\{b_i, P_i, R_i, \perp, x_i, r_i, 1\}$ 添加到 L_4，并返回 $\{P_i, R_i, \perp, x_i\}$。此事件被定义为 E_1。

(2) 否则，B 随机选择 x_i，d_i，$\alpha_i \in Z_q^*$，计算 $P_i = x_i \cdot P$ 以及 $R_i = d_i P(\alpha_i P_0) - 1$，并定义 $h_0(a_i, R_i) = \alpha_i$。然后，B 将 $\{b_i, R_i, \alpha_i\}$ 和 $\{b_i, P_i, R_i, \perp, x_i, r_i, 0\}$ 分别添加至 L_0 和 L_4 中，并返回 $\{P_i, R_i, d_i, x_i\}$。

此外，A_1 可以取代公钥 P_{b_i}。

挑战：A_1 将 $\{m_0, m_1, \mathrm{rcv}_0, \mathrm{rcv}_1, a_0, a_1\}$ 发送给 B，其中 $\mathrm{rcv}_0 = b_0$，$\mathrm{rcv}_1 = b_1$。B 分别从 L_3 和 L_4 获得 $\{a_i, P_i, R_i, d_i, x_i\}$ 和 $\{b_i, P_i', R_i', d_i', x_i', r_i', c_i\}_{i=0,1}$。

(1) 如果 $c_0 \neq 1$，$c_1 \neq 1$，B 则终止，此事件定义为 E_2。

(2) 否则，B 随机选择 $v \in \{0, 1\}$，$V \in \{0, 1\}^l$，并定义 m_v 的密文为 $C = (zP, V)$。最后，B 将密文 $C = (zP, V)$ 发送给 A_1。

猜测：A_1 返回 v'。如果 $v = v'$，B 输出 1，否则，B 输出 0。同时，B 从 L_2 中随机选择一个元组 $\{X_i, h_{2,i}\}$ 并输出 $D = abP = (X_i(br_v') - 1)\, 1/\alpha_v'$。

设定 E_3 代表事件 A_1 在模拟中的某个时间点上查询 $h_2((bP) r_v' D^{\alpha_i'})$。由于 $\Pr[\neg E_1] = \delta^{q_R}$ 及 $\Pr[\neg E_2] = (1-\delta)^2$，可以得知，$\Pr[\neg E_1 \wedge \neg E_2] = \delta^{q_R}(1-\delta)^2$，当 $\delta = q_R/(q_R+2)$ 时取得最大值 $4/(e^2(q_R+2)^2)$，其中 q_R 表示 A_1 查询加密密钥生成的最大次数。

分析：当 $\Pr[E_3] \geqslant 2\varepsilon$，$B$ 可以 $\varepsilon' \geqslant 8\varepsilon/(e^2(q_R+2)^2 q_{h_2})$ 的优势解决 CDH 问题，其中 q_{h_2} 表示 A_1 查询 h_2 的最大次数。这与已知的 CDH 困难性假设的困难性相悖。

引理 2：假设敌手 A_2 以不可忽略的优势 ε 攻破本方案，那么一个构建的算法 B 则可以优势 $\varepsilon' \geqslant 8\varepsilon/(e^2(q_R+2)^2 q_{h_2})$ 解决 CDH 困难性问题。

该引理的证明思路同引理 1 类似。

6 性能分析

本节将本方案与现有方案从特征、计算开销和时间消耗三方面进行对比分析。

6.1 特征对比

本方案与现有的双边访问控制方案[9-10]的特征对比如表 2 所示。文献[9]提出了一个基于双线性配对的访问控制方案 ME，其密钥生成过程依赖于可信第三方实体，导致了复杂的密钥托管问题。针对这一问题，文献[10]基于无证书加密技术构建了两个无密钥托管的访问控制方案，一是采用双线性配对技术的基础方案 BS，二是避免配对操作的轻量级方案 LS。而本方案在避免密钥托管和配对操作的基础上，将部分加密和解密过程外包给边缘服务器，减少了终端的计算压力。

6.2 计算开销

本节将对本方案与现有方案的计算开销进行比较分析。表 3 首先给出了对比中涉及的关键操作的符号及其描述。其中，G_T 为 ME 方案[9]和 BS 方案[10]中一个阶为 q 的循环群，其满足双线性映射 e：$G \times G \rightarrow G_T$。鉴于 Z_q^* 上的运算与普通的哈希操作的计算开销相对较小，其在整体计算开销中的影响可以忽略不计，在进行对比分析时，仅对关键操作进行对比。

表 2　特征对比

方案	无密钥托管	无配对计算	外包加/解密
ME 方案[9]	否	否	否
BS 方案[10]	是	否	否
LS 方案[10]	是	是	否
本方案	是	是	是

表 3　性能分析的符号

符号	描述
BP	双线性配对运算
M_{G_T}	G_T 上的乘法运算
H_G	映射到群 G 的哈希运算
M_G	群 G 上的乘法运算
A_G	群 G 上的加法运算

表 4 给出了本方案与 ME 方案[9]、BS 方案[10]、LS 方案[10]在不同阶段的计算开销。在加密密钥生成和解密密钥生成阶段，ME 方案和 BS 方案涉及到了 M_G 和 H_G 操作，而 LS 方案和本方案仅涉及 M_G 的操作。由于本方案在此阶段对部分密钥的正确性进行了验证，因此，计算开销略高于 LS 方案。ME 方案和 BS 方案因采用双线性配对技术，且与本方案相比额外涉及 H_G 和 M_{G_T} 操作，导致其在加密和解密阶段的计算开销较大。此外，本方案将部分加密、解密外包给边缘服务器减少了终端的计算开销。与同为无配对操作的 LS 方案相比，本方案在加密阶段的计算开销减少了 $M_G + A_G$，在解密阶段的计算开销减少了 $2M_G + 2A_G$。

6.3　仿真实验

为进一步进行对比分析，本节将本方案与 ME 方案、BS 方案、LS 方案在各个阶段的时间消耗进行对比。实验环境基于 Windows 10 64 位操作系统，Intel（R）Core（TM）i5 - 8250U@ 1.6GHz 处理器，并选择椭圆曲线 $y^2 = x^3 - 3x$ 进行仿真。各个阶段分别运行 10、20、30、40 和 50 遍，对其消耗的时间进行记录，实验结果取 10 次实验的平均值。图 6 ~ 图 9 分别显示了加密密钥生成、解密密钥生成、加密及解密阶段的时间消耗。

表 4　计算开销的对比

方案	加密密钥生成	解密密钥生成	发送端加密	接收端解密
ME 方案[9]	$M_G + H_G$	$2M_G + 3H_G$	$2BP + 3M_G + H_G + A_G$	$3BP + H_G + M_{G_T}$
BS 方案[10]	$2M_G + H_G$	$3M_G + 2H_G$	$2BP + 2M_G + H_G + 3A_G$	$4BP + 2M_G + 2H_G + A_G + 2M_{G_T}$
LS 方案[10]	$2M_G$	$2M_G$	$4M_G + A_G$	$4M_G + 2A_G$
本方案	$3M_G$	$3M_G$	$3M_G$	$2M_G$

图 6 呈现了本方案与 ME 方案、BS 方案、LS 方案在加密密钥生成阶段的时间消耗。通过实验发现执行一次 H_G 操作的时间约为执行一次 M_G 操作时间的 2.3 倍。因此，在此阶段包含 H_G 操作的 ME 方案和 BS 方案的时间消耗均高于本方案。由于本方案为了确保部分密钥的正确性对其进行了验证，因此本方案在此阶段的时间消耗略大于 LS 方案。

图 7 展示了本方案与现有方案在解密密钥生成阶段的时间消耗对比。在此阶段，ME 方案和 BS 方案的时间消耗取决于执行 M_G 和 H_G 的时间，而 LS 方案与本方案与执行 M_G 的时间相关。因此，ME 方案和 BS 方案的时间消耗较为接近，且显著高于 LS 方案和本方案。此外，本方案在此阶段同样增加了对部分密钥的验证，导致其时间消耗略高于 LS 方案。

图 8 为发送端加密阶段的时间消耗对比。在此阶段，ME 方案和 BS 方案采用双线性配对技术，其单次 BP 的时间消耗约为 15.141 ms。BS 方案和 LS 方案[20]的时间消耗还包含 A_G 操作，执行一次的时间约为 0.046 ms。由于执行 BP 的时间远远大于执行 M_G，故 ME 方案和 BS 方案的时间消耗超过 LS 方案和本方案。此外，本方案将部分加密外包给了边缘服务器，减少了发送端的解密时间，使得本方案的时间消耗略低于 LS 方案。

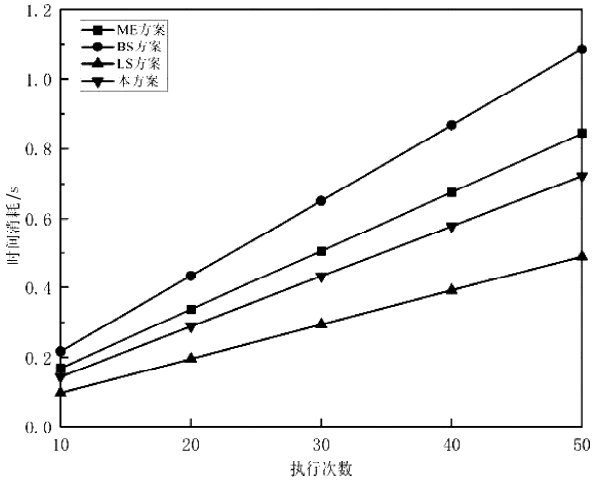

图 6　加密密钥生成阶段的时间消耗

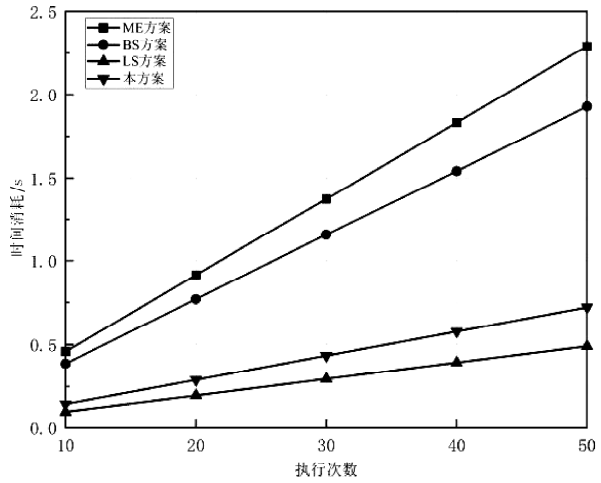

图 7　解密密钥生成阶段的时间消耗

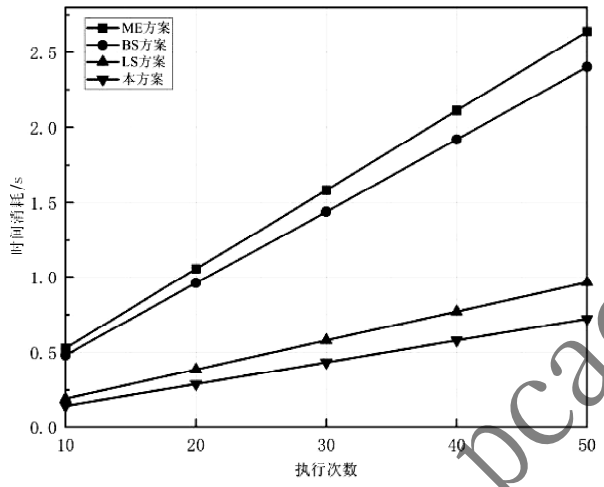

图 8　发送端加密的时间消耗

图 9 为接收端解密阶段的时间消耗。在此阶段，BS 方案执行 BP、H_c 和 M_c 操作的次数均多余 ME 方案，而执行 M_{G_T}的时间消耗约为 0.008 ms，时间消耗较小，因此，BS 方案的时间消耗大于 ME 方案。本方案的计算开销不涉及耗时较多的 BP 操作，时间消耗也远低于 ME 方案和 BS 方案。此外，本方案将部分解密操作外包给边缘服务器，减少了接收端解密的计算负担，从而使得本方案的时间消耗略小于 LS 方案。

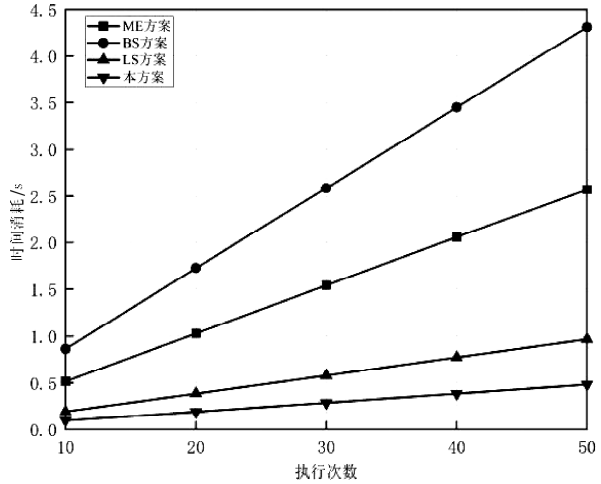

图 9　接收端解密阶段的时间消耗

综上所述，在加密密钥生成和解密密钥生成阶段，本方案的时间消耗虽略多于 LS 方案，但远小于 ME 和 BS 方案，呈现出轻量级的使用效果。而在加密和解密阶段，由于本方案避免了双线性配对操作且采取外包加解密，使得本方案终端设备的时间消耗均小于现有方案，体现出较强的使用性。

7　结论

针对卫星物联网环境，本方案基于无证书加密技术和匹配加密技术提出了一种无证书双边访问控制方案。本方案不仅有效地避免了传统加密技术的密钥托管和证书管理问题，还实现了对发送端和接收端双边访问控制。此外，本方案选择椭圆曲线密码作为加解密方式，避免了耗时较大的双线性配对操作，并将部分加密和解密过程外包给边缘服务器，显著降低了终端设备的计算负担。安全性分析证明本方案的正确性与安全性，性能分析表明，与现存方案相比，本方案具有更高的计算效率。

参考文献

[1] 李庭瑞，李锐，罗睿，等. 基于 IPK 的电力卫星物联网安全接入研究 [J]. 电力信息与通信技术，2021，19（4）：70－75.

[2] AL－RIYAMI S S，PATERSON K G. Certificateless public key cryptography [C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin，Heidelberg：Springer Berlin Heidelberg，2003：452－473.

[3] KUMARI D，SINGH K. Lightweight secure authentication and key agreement technique for smart grid [J]. Peer-to-Peer Networking & Applications，2024，17（1）：451－478.

[4] DENG L，GAO R. Certificateless two-party authenticated key agreement scheme for smart grid [J]. Information Sciences，2021，543：143－156.

[5] CUI W，CHENG R，WU K，et al. A certificateless authenticated key agreement scheme for the power IoT [J]. Energies，2021，14（19）：6317.

[6] CHEN Y，LI J，LIU C，et al. Efficient attribute based server-aided verification signature [J]. IEEE Transactions on Services Computing，2021，15（6）：3224－3232.

[7] ELHOSENY M，SHANKAR K. Reliable data transmission model for mobile ad hoc network using signcryption technique [J]. IEEE Transactions on Reliability，2020，69（3）：1077－1086.

[8] SUN J，XU G，ZHANG T，et al. Privacy-aware and security-en-

hanced efficient matchmaking encryption [J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 4345 - 4360.

[9] ATENISES G, FRANCATI D, NUNEZ D, et al. Match me if you can: matchmaking encryption and its applications [J]. Journal of Cryptology, 2021 (34): 1 - 50.

[10] WU A, LUO W, WENG J, et al. Fuzzy identity-based matchmaking encryption and its application [J]. IEEE Transactions on Information Forensics and Security, 2023.

[11] NAYAK P, SWAPNA G. Security issues in IoT applications using certificateless aggregate signcryption schemes: an overview [J]. Internet of Things, 2023 (21): 100641.

[12] ALI I, CHEN Y, ULLAH N, et al. Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2021, 70 (6): 5974 - 5989.

[13] KARATI A, FAN C I, ZHUANG E S. Reliable data sharing by certificateless encryption supporting keyword search against vulnerable KGC in industrial Internet of Things [J]. IEEE Transactions on Industrial Informatics, 2021, 18 (6): 3661 - 3669.

[14] ZHANG Y, LIU X, LANG X, et al. VCLPKES: verifiable certificateless public key searchable encryption scheme for industrial Internet of Things [J]. IEEE Access, 2020 (8): 20849 - 20861.

[15] MA M, LUO M, FAN S, et al. An efficient pairing-free certificateless searchable public key encryption for cloud-based IIoT [J]. Wireless Communications and Mobile Computing, 2020, 2020 (1): 8850520.

[16] LIU X, DONG H, KUMARI N, et al. A pairing-free certificateless searchable public key encryption scheme for industrial Internet of Things [J]. IEEE Access, 2023, (11): 58754 - 58764.

[17] ELHABOB R, TAHA M, XIONG H, et al. Pairing-free certificateless public key encryption with equality test for Internet of Vehicles [J]. Computers and Electrical Engineering, 2024, 116: 109140.

[18] FRANCATI D, GUIDI A, RUSSO L, et al. Identity-based matchmaking encryption without random oracles [C]//International Conference on Cryptology in India. Cham: Springer International Publishing, 2021: 415 - 435.

[19] CHEN J, LI Y, WEN J, et al. Identity-based matchmaking encryption from standard assumptions [C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer Nature Switzerland, 2022: 394 - 422.

[20] CHEN B, XIANG T, MA M, et al. CL-ME: efficient certificateless matchmaking encryption for Internet of Things [J]. IEEE Internet of Things Journal, 2021, 8 (19): 15010 - 15023.

[21] YANG N, TANG C, HE D. A lightweight certificateless multi-user matchmaking encryption for mobile devices: enhancing security and performance [J]. IEEE Transactions on Information Forensics and Security, 2023, 19: 251 - 264.

[22] YAN Y. The overview of elliptic curve cryptography (ECC) [C]// Journal of Physics: Conference Series. IOP Publishing, 2022, 2386 (1): 012019.

[23] FILIPPONE G. On the discrete logarithm problem for elliptic curves over local fields [J]. arXiv preprint arXiv: 2304.14150, 2023.

[24] 向宴颉, 黄晓芳, 向科峰, 等. 一种基于国密算法的区块链无证书加密机制 [J]. 计算机科学, 2024, 51 (8): 440 - 446.

[25] DENG L, FENG S, CHEN Z. Certificateless encryption scheme with provable security in the standard model suitable for mobile devices [J]. Information Sciences, 2022, 613: 228 - 238.

[26] DAI C, XU Z. Pairing-free certificateless aggregate signcryption scheme for vehicular sensor networks [J]. IEEE Internet of Things Journal, 2022, 10 (6): 5063 - 5072

(收稿日期: 2024 - 12 - 10)

作者简介:

张华乐 (1991 -), 男, 硕士研究生, 工程师, 主要研究方向: 电力系统通信。

陆俊 (1983 -), 男, 硕士研究生, 高级工程师, 主要研究方向: 电力系统通信。

林航 (1975 -), 男, 本科, 高级工程师, 主要研究方向: 电力系统通信。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部