文章编号：2095-2163(2022)12-0110-05 中图分类号：TP309.2 文献标志码：A

基于椭圆曲线加密算法的工业物联网数据隐私保护方案

冯云霞，王西贤
（青岛科技大学 信息科学技术学院，山东 青岛 266061）

摘 要：目前，通过工业物联网不同类型的工业设备实现集群交互，打破了数据孤岛，使得数据不再是独立的，但在这种情况下，数据的传输伴随着数据泄露这一安全问题。此外，工业物联网还表现出需要去中心化、可追溯等特点。为了解决这一问题，本文提出了一个在区块链架构下的基于椭圆曲线加密算法的工业物联网数据隐私保护方案。在方案中，数据接收者和数据发送者之间的数据通过一次性密码进行加密。同时，方案中的密钥传输、密文传输等均由智能合约进行管理，加解密过程均在本地操作，减少智能合约的计算消耗。最后，方案经过仿真及安全性分析，确保方案能实现数据隐私保护。

关键词：椭圆曲线；数据隐私；工业物联网；区块链；一次性密码

Data privacy protection scheme of industrial Internet of Things based on elliptic curve encryption algorithm

FENG Yunxia, WANG Xixian
(College of Information Sceince and Technology, Qingdao University of Science and Technology, Qingdao Shandong 266061, China)

【Abstract】 At present, the cluster interaction of different types of industrial equipments through the Industrial Internet of Things breaks the data silos, so that the data is no longer independent, but in this case, the transmission of data is accompanied by the security problem of data leakage. In addition, industrial objects networking also needs features such as decentralization and traceability. In order to solve this problem, this paper proposes an industrial IoT data privacy protection scheme based on elliptic curve encryption algorithm under the blockchain architecture. In the scheme, the data between the data receiver and the data sender is encrypted by a one-time password. Meanwhile, the key transmission and ciphertext transmission in the scheme are managed by smart contracts, and the encryption and decryption processes are operated locally, reducing the computational consumption of smart contracts. Thereafter, through simulation and security analysis, it is ensured that the scheme can achieve data privacy protection.

【Key words】 elliptic curve; data privacy; industrial Internet of Things; blockchain; one-time password

0 引 言

随着各种技术的发展，大数据、云计算以及物联网(Internet of Things，IoT)等创新理念的兴起，也随即将现代产业提升到一个新的高度[1]。在此情况下，工厂借助传统工业平台和新型的技术，进行深度的融合与集成，强化在工业终端方面的互联互通，打造工业领域的物联网，实现泛在感知条件下的智能化制造，最大化地提升行业生产效率，这就是工业物联网(Industrial Internet of Things，IIoT)。通过工业物联网，工厂中不同类型的工业设备实现集群交互，打破了数据孤岛，使得数据不再是独立的。通过数据之间的碰撞与融合，推动制造过程的智能化、网络化转型升级[2]。

通过工业物联网，工业已进入蓬勃发展时期。然而，随着节点数量和网络规模的增加，传统的云服务平台下的工业物联网已经不能为如此庞大的系统提供有效的支持。一方面，在平台上共享数据将消耗大量带宽资源，导致数据共享成本增加。另一方面，平台上的数据在传输工程中也很容易被泄露，由于工业数据的高敏感性，数据泄露的后果极其严重。此外还会看到，共享数据应是易于验证的，以防止重要数据被篡改，这是传统的云服务平台无法保证的。

因此，研究拟在工业物联网中引入了区块链架构，这是一种新兴的分布式网络构建方案，以重塑传统的云平台工业物联网架构。区块链技术是比特币的底层技术之一，会生成多个相链接的数据块，其中每个里面都包含重要信息，以验证其有效性，并生成下一个数据块。区块链作为一个分布式数据库，具有不可篡改、隐私保护和去中心化等特点[3]，有助于建立安全的数据共享机制，区块链具有实现工业物联网产生的工业大数据安全数据共享的潜力。

作者简介：冯云霞(1977-)，女，博士，副教授，主要研究方向：物联网与应用技术、大数据安全与隐私保护技术；王西贤(1997-)，女，硕士研究生，主要研究方向：区块链、工业物联网。

收稿日期：2022-03-21

本文提出了一个基于椭圆曲线加密算法的工业物联网数据隐私保护方案，该方案基于以太网联盟链的数据共享框架，通过智能合约对用户进行管理以及业务逻辑的监督，并通过区块链网络为数据共享做准备。为了确保数据在链上传输的安全，采用传统的数据的隐私保护方法来加密数据，利用一次性椭圆曲线加密算法对数据进行加密，从而切实保障了数据传输中的数据隐私。

1　相关工作

数据作为工业互联网的核心要素，从最开始的终端收集到存储以及后续的数据流转都面临着风险，尤其是在传输的过程中，保证数据不致泄露、被篡改是至关重要的。目前，陆续提出了多种关于在区块链架构下数据传输过程中保障数据隐私安全的技术方案。

区块链作为一种新兴的技术，将密码学、共识机制、分布式存储融合在一起，是一种不可更改、不可伪造的分布式数据库，有着去中心化、防篡改、可溯源等工业物联网安全所需要的特点[4]。在加密货币零币[5]中，使用传统的加密方式来对交易内容进行隐藏，在不泄露任何交易内容的前提下，只有发送方和接收方获知交易金额，其它任何人无法得知具体的交易面额。Linder[6]提出了一套数据解密密钥管理系统，采用加密的智能合约，通过公私钥方式保护公共隐私文件。Gai 等人[7]提出了一种将物联网与边缘计算和区块链相结合的新方法，即基于区块链的边缘互联网(BIoE)模型。充分利用边缘计算、差分隐私保护和区块链的优势建立隐私保护机制，提出的模型以节能的方式在不降低性能的情况下提高了隐私保护。Prajapati 等人[8]提出了生成多个密钥的关键块链接方法，生产密钥块用于单个明文块的加密。Hammi 等人[9]扩展了一次性密码(One Time Password，OTP)的概念，并用其来生成一个新的密钥，用于物联网设备和服务器之间的每次交换，提出了一种基于椭圆曲线密码(Elliptic Curve Cryptography，ECC)的 OTP 生成方法，以确保物联网的安全性。

2　数据隐私保护方案概述

在前文研究论述基础上，本文提出了一种适用于区块链架构下工业物联网中的节点数据隐私保护方案。首先指出区块链架构下工业物联网中节点数据的交换方式，根据实际情况，利用传统的数据隐私保护方法、即数据加密来保护数据隐私安全，然后根据工业物联网数据量大、数据操作频繁等特点，采用一次性密码生成加密密钥对数据进行加密，并结合区块链特点，构建区块链架构下适用于工业物联网的节点数据隐私保护方案。最后给出方案设计及安全性分析。

2.1　面临的挑战

对于工业物联网中的节点数据隐私保护方案需要解决以下 3 个问题。一是节点之间的身份确认，二是节点数据的保护，三是节点数据的完整性验证。对此可做阐释论述如下。

(1)对于节点之间的身份确认问题。区块链作为一个去中心化的平台可以通过智能合约得到解决。在联盟链的架构下，用户想要加入链内、访问信息，需要经过联盟链中管理员的许可，这样就在一定程度上确保了节点的身份。

(2)对于数据保护问题。常用的加密技术有 2 种，即对称加密算法和非对称加密算法[10]。在对称加密算法中，由于对明文的加密和密文解密使用相同的密钥，因此要保证密钥传输的安全，确保密钥不被泄露。而在非对称加密算法中，采用公钥加密、私钥解密的方式，公钥公开、私钥保密，无需像对称加密一样保证密钥安全传输。在这种情况下，加密和解密使用的密钥并不相同，在数据传输环境不太信任的情况下具有较大的安全优势，与对称加密相比，非对称加密可以较好地保证私钥的安全，确保数据不被泄露。

但是，一直使用相同的密钥可能会导致严重的安全问题。为了应对这一安全风险，本文再次将 OTP 的概念拓展开来。在每次进行数据传输前由数据接收者生成一个新的密钥，发送给数据发送者，让数据发送者用于本次两者之间的数据传输。

(3)对于数据的完整性验证。安全哈希算法是一种迭代的、单向的哈希函数，可以将消息通过处理生成称为消息摘要的一种压缩算法[11]。这种算法可以确定消息的完整性，并且对消息的任何更改都将极有可能生成不同的消息摘要。

安全哈希算法有很多种，输出的结果称为消息摘要。消息摘要的长度从 160~512 位不等，具体取决于所采用的算法。安全哈希算法通常与其他加密算法一起使用，例如数字签名算法和键控哈希消息验证码，或者在随机数的生成中使用。哈希算法之所以被称为安全算法，是因为对于给定的算法来说，在计算上是不可行的：

(1)找到与给定消息摘要相对应的消息。

(2)找到产生相同消息摘要的 2 个不同消息。

对消息的任何更改都极有可能产生不同的消息摘要。其中,SHA-256 算法由于在散列或消息摘要大小期间使用的块和数据字的大小方面有着强大优势,因此采用 SHA-256 算法。

2.2 数据隐私方案概述

在本方案中,数据发送者与数据接收者均属于联盟链成员,数据接收者向数据发送者共享一个一次性密码的公钥,数据发送者收到后对数据加密得到密文和摘要,再将摘要发送给数据接收者。这样就完成了一次安全的数据共享。

该方案可以分为 4 个主要阶段,依次为:一次性密钥生成、密钥获取及数据加密、数据发送和数据接收与验证,整个数据隐私方案的设计流程如图 1 所示。数据从数据发送者到数据接收者之间的转移流程拟展开研究分述如下。

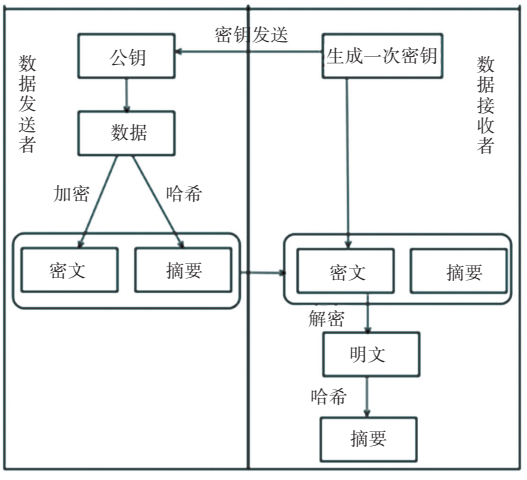

图 1 数据隐私方案流程图

Fig. 1 Flow chart of data privacy scheme

(1)一次性密钥生成阶段:数据接收者在本地生成一个一次性的公私钥对,该公私钥对由椭圆曲线加密算法生成。椭圆曲线加密算法相比于 RSA 和 DSA 算法速度更快,存储空间占用小,带宽要求低,安全性高。通过这样一个一次性的公私钥对可以有效提高数据的安全性。公钥可以直接通过智能合约发送给数据发送者,无需做过多的防护。

(2)密钥获取及数据加密阶段:数据发送者在接收到公钥后对需要发送的数据进行加密得到密文;再将原始数据进行哈希计算得到一个摘要。

(3)数据发送阶段:将(2)中所得的密文和摘要发送给数据接收者。

(4)数据接收与验证阶段:数据接收者在收到密文和摘要后,先用私钥对密文进行解密,得到明文,再将明文进行哈希计算得到摘要与收到的摘要做对比,若相等,则证明数据完整,安全可信。

3 数据隐私保护方案实现

3.1 算法实现

根据上文的描述可以得知,数据隐私方案主要包含 4 个算法。算法中,secp256k1 曲线的参数如下:E 代表椭圆曲线 secp256k1,其有限域为 $F(p)$。G 是曲线 E 的循环子群,生成元是 P,其阶是 n。这里可给出重点论述如下。

(1)一次性密钥生成算法:数据接收者在本地生成一个一次性的公私钥对,该公私钥对由 secp256k1 曲线生成。在给定的曲线 secp256k1 上,随机输入一个合法私钥 d,$d \in [1,n-1]$,此时将输出:

$$K = dG \tag{1}$$

(2)椭圆曲线加密算法:数据发送者在接收到公钥 K 后对需要发送的数据 M 进行加密得到密文 C;选取随机数 r,$r \in [1,n-1]$,具体可经由如下公式进行计算:

$$c_1 = rG = (x_1, y_1) \tag{2}$$

$$c_2 = rK + M \tag{3}$$

则密文 C 就是(c_1, c_2)。

(3)椭圆曲线解密算法:数据接收者在收到密文 (c_1, c_2) 后,用私钥对密文进行解密,得到明文,推得的公式可写为:

$$c_2 - d\,c_1 = M \tag{4}$$

(4)SHA-256 安全哈希函数算法:数据发送者对需要发送的数据进行哈希计算;数据接收者对解密后的明文也要进行哈希计算。将数据输入后,经过预处理和哈希计算两个阶段后输出 256 位的消息摘要。

3.2 智能合约的实现

该方案的实现需要通过智能合约来对业务逻辑进行管理。数据接收者将公钥上传的同时要包含数据发送者的地址,这样数据发送者便能根据数据发送者自己的地址查询到加密公钥;同理,数据发送者在上传数据的时候也要加上数据接收者的地址,以便数据接收者根据自己的地址和加密公钥查询到数据。这都需要智能合约进行管理。

合约的目的是管理数据共享者与数据接收者,该合约针对不同的主体:数据发送者和数据接收者,各有 2 个功能函数,具体见表 1。

表 1　数据分享合约中函数功能说明表

Tab. 1　Functions description table in the data sharing contract

函数名称	函数说明
getdatapack	获取数据
addpk	上传加密公钥
addatapack	上传数据
getpk	获取加密公钥

其中，*addpk*，*getdatapack* 是数据接收者所调用的函数；*addatapack*，*getpk* 则是数据发送者所调用的函数。数据发送者和数据接收者指的是在一次数据分享中的 2 个用户之间，而并不是一个用户只能是数据接收者或只能是数据发送者，二者并不是一成不变的。

4　实验结果及分析

4.1　实验环境

本文的实验环境如下：在 Windows 10 的操作系统下，在 Ubuntu 虚拟机中使用 FISCO BCOS 企业级金融联盟链底层平台和微众银行开源的自研区块链中间件平台 WeBASE 平台，在本地搭建起一个联盟链，通过 solidity 语言来编写智能合约，进行仿真实验，验证方案的可行性。在实验中将模拟数据接收者从生成一次性密钥直至接收到密文的哈希验证阶段，并在最后给出了方案的安全性分析。

4.2　实验结果

将本地联盟链启动，启动多个节点做好准备工作，再将数据隐私保护方案所需智能合约进行上链部署，并进行数据分享。在数据接收者上传了公钥、数据发送者接收了公钥、并上传数据后，进行查询。对预期结果和实验结果分别做出解析概述如下。

（1）预期结果：根据加密公钥和数据接收者地址信息查询到数据。

（2）实验结果：返回数据发送者上传的数据。如图 2 所示。图 2 中显示的是查询结果。根据图 2 中的交易回执，message：“Success”说明合约正常执行，通过查询，返回一个 output，可以获得一个密文及一个摘要。其中，content 为加密后的明文，zhaiyao 则是明文通过哈希计算的值。

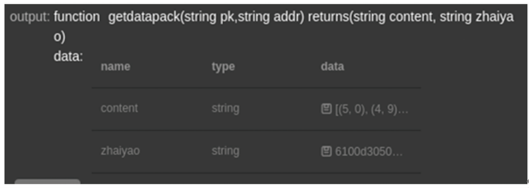

图 2　数据查询回执

Fig. 2　Data query receipt

下一步进行密文解密，输入加密公钥和与之对应的私钥、以及密文，对数据进行解密。对得到的明文进行哈希计算，得到摘要，与收到的 zhaiyao 相对比。对预期结果和得到的实验结果将分别给出评析综述如下。

（1）预期结果：密文解密后得到明文，对明文的哈希计算结果与收到的 zhaiyao 相同。

（2）实验结果：实验结果如图 3、图 4 所示。哈希值对比详见表 2。

图 3　密文解密

Fig. 3　Decryption of ciphertext

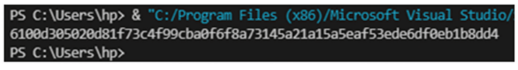

图 4　明文的哈希计算结果

Fig. 4　Hash calculation result of plaintext

表 2　哈希值对比

Tab. 2　Hash value comparison

对照项	对照值
收到的哈希值	6100d305020d81f73c4f99cba0f6f8a73145a21a15a5eaf53ede6df0eb1b8dd4
本地计算哈希值	6100d305020d81f73c4f99cba0f6f8a73145a21a15a5eaf53ede6df0eb1b8dd4

通过表 2 可以发现，在对解密后明文进行哈希计算后所得结果值与收到的摘要相等，说明数据从数据发送者到数据接收者是一样的，数据是完整的。

假设其他节点从数据发送者到数据接收者之间的通信中收集到加密公钥 P 和密文 C，然后试图从密文 C 中获得消息 M。但是要想解密密文 C 必须要知道私钥 d，$P = d * G$，这种攻击是不可能的，因为攻击者需要面对椭圆曲线离散对数的困难。因此，第三方攻击并不适用于所提议的方案。

其他节点虽然在知道公钥和数据接收者地址的情况下也可获得密文，但因为不知道私钥将无法解密密文，就不能得知数据，防止了数据的泄露。

5　结束语

通过对工业物联网数据的隐私保护可以有效提

（下转第 121 页）