ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 37,No. 6,Nov. 2022,pp. 1314－1322
DOI:10. 16337/j. 1004-9037. 2022. 06. 012

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

一种基于区块链的保密文件同城寄递自适应路径规划算法

周　倩[1]，张添龙[1]，吴加洋[1]，韩忠旭[1]，戴　华[2]

(1. 南京邮电大学现代邮政学院,南京 210003;2. 南京邮电大学计算机学院,南京 210023)

摘　要：为了解决保密文件同城寄递效率低和隐私泄露问题,本文设计了一种基于区块链的同城路径规划算法,自适应地实时生成一条保护位置隐私的寄递最短路径。系统利用区块链的共识机制和智能合约算法,通过同态加密选择规划路线中各分布式站点。车辆利用自身上下文信息才可以加解密下一条站点信息,具有防冒充的功能。该算法也解决了车辆、站点和快递员之间互不信任的问题。最后通过原型系统的测试,针对智能合约同态计算结果、不同上下文属性个数,和不同站点个数对路径规划计算代价影响进行了分析。实验结果表明保密文件同城寄递系统中的路径规划算法具备机密性、完整性和防篡改的功能,保证了高寄递效率。

关键词：区块链;同城寄递;智能合约;同态加密

中图分类号：TP301　　**文献标志码**:A

An Adaptive Path Planning Algorithm for Local Delivery of Confidential Documents Based on Block-Chain

ZHOU Qian[1], ZHANG Tianlong[1], WU Jiayang[1], HAN Zhongxu[1], DAI Hua[2]

(1. School of Modern Posts, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;2. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Targeting the low efficiency and privacy leakage of intra-city delivery of confidential documents, a intra-city path planning algorithm based on block-chain is proposed. It adaptively generates the shortest path to protect location privacy in real time. With the consensus mechanism and smart contract algorithm of block-chain, the distributed site is selected by route planning with homomorphic encryption. The vehicle can encrypt and decrypt the next site information by using its own context attribute, and be equipped with anti-impersonation. This algorithm also solves the problem of mutual distrust among vehicles, sites and deliveries. Finally, through experiments, the impact of the homomorphic calculation results of smart contracts, the number of different contextual attributes, and the number of different sites on the calculation cost of path planning is analyzed. The results show that the algorithm of the intracity delivery system has the capabilities of confidentiality, integrity and anti-tampering and can ensure high-delivery efficiency.

Key words: blockchain; intra-city delivery; smart contract; homomorphic encryption

---

基金项目:国家自然科学基金(61902199,61872197,61972209)。
收稿日期:2022-07-18;**修订日期**:2022-08-28

引　言

近年来,一些党政机关或涉密单位通过普通邮政传递国家保密文件,可能存在可靠性差、可控性差且扩大知悉范围等危害。中华人民共和国保守国家秘密法第3章第25条指出:不得通过普通邮政、快递等无保密措施的渠道传递国家秘密[1]。但是,目前邮政企业并没有对寄递的机要文件有严格的监管措施。对于企业(如会计、法律、研究所和券商等)而言,合同、资质、发票、报告和证件等重要商务文件的运输过程,需要较高的机密性、快速性与动态性,订单信息需要具备防篡改、防冒充的能力。现有的方案为一个订单由一个专人配送或通过机要文件交换站进行交换,所有信息由单个云系统维护,成本高昂,难以持续发展[2]。与城市间的主干道相比,同城配送中道路交通更为复杂。出于对寄递效率与服务质量的考虑,无论是邮政企业,还是普通物流企业,同城配送背景下保密文件的寄递效率与安全都迫切需要提升,保密文件的寄递问题迫切需要一种解决方案。

全同态加密的概念于1978年首次被Rivest等[3]提出,它允许直接对密文进行运算处理,其输出结果与对明文进行同样的运算处理再将结果进行加密相同。同年,Rivest等[4]提出了RSA(Rivest-Shamir-Adleman)算法,其安全性依赖于数论中大数分解的困难性,密钥越长安全性越高,因此,它的计算量大,加密速度比较慢,作为一个同态加密算法,其仅具有乘法同态性,并不具有加法同态性。1999年,Paillier[5]基于复合剩余类的困难问题发明了Paillier加密算法,其仅满足加法同态,并不满足乘法同态。Gentry等[6-8]于2009年基于理想格数学结构第1次提出了全同态加密算法,从此全同态加密被重视起来。基于全同态加密算法运算复杂和效率较低等特点,国内外的学者都提出了自己的改进方案。全同态加密算法可以对密文直接进行运算,得到的结果与明文运算效果一样。

近年来,区块链技术因其分布式记账和去中心化、不可篡改等特点,被许多领域看好。区块链采用了Hash算法、公钥密钥密码学以及零身份证明等相关密码学技术[9],链上存储结构Merkle哈希树可以验证数据完整性,因此它在物流行业保护信息的完整性、机密性和隐私性有着广泛的应用。譬如,京东全球购的全链条采用区块链溯源技术,顾客可以查看到寄递的时间、运输路线和方式等信息。为了加强寄递的机密性,需要对寄递信息进行进一步机密性处理,确保在整个寄递过程中的安全性。车辆只有在配送的过程中才具备的属性信息叫车辆上下文信息(Contextual information),比如车辆的速度、车辆抵达的时间、站点位置等[10-11]。利用车辆的上下文信息将下一条站点的信息进行属性加密,可以抵御车辆被冒充非法取得保密文件,即使快递员(车辆)被捕获,攻击者无法获得正确的身份信息、合法位置、合法时间等属性解密下一跳站点。

从同城寄递行业发展的视角来看,快递路径一次性规划难以适应同城配送中道路交通复杂的情况,此外,车辆、站点和快递员之间互相不信任导致的矛盾也与日俱增,隐私泄露问题频出[12]。针对以上现状,本文设计了一种基于区块链的保密文件同城寄递自适应路径规划算法,实时生成一条保护位置隐私的最短路径,满足当前同城保密文件寄递响应敏捷、保护安全隐私的要求。最后通过原型系统的测试,对智能合约同态计算结果、上下文属性个数和站点个数对路径规划计算代价影响进行了分析,实验结果表明保密文件同城寄递系统具备寄递信息的机密性、完整性和防篡改的功能,保证了寄递的高效率。

1　保密文件同城寄递系统架构

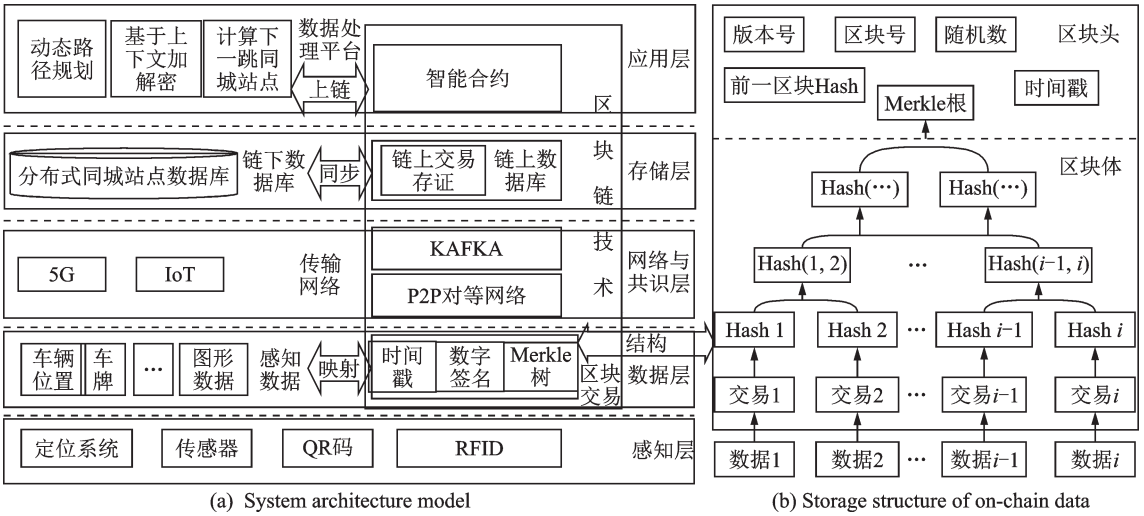
基于区块链去中心化、分布式节点间互相平等的特点和同城寄递场景下站点之间不区分上下级的现实情况,区块链技术在同城寄递场景下具有天生的优势,减轻了消息传递至云端的通信成本。本系

统利用分布式运算、实时动态生成快递运输路径，假设载有保密文件的车辆此时到达站点S_i，站点S_i需要从多个可能的下一跳站点中选择一个距离终点S_d最近的站点，为了防止站点位置隐私的泄露，对所有可能的下一跳站点与终点S_d进行同态加密$F()$后进行运算，得各站点与终点之间的距离Distance。求下一跳站点即求满足以下要求的站点S_{i+1}。

$$S_{i+1}=\mathrm{Min}\{\mathrm{Distance}(F(S_0),F(S_d)),\mathrm{Distance}(F(S_1),F(S_d)),\cdots,\mathrm{Distance}(F(S_{n-1}),F(S_d))\} \tag{1}$$

当前S_i站点抵达终点S_d最短路径为$(S_i,S_{i+1},\cdots,S_d)$。系统感知数据主要来源于车辆采集、站点实时生成的数据。为了保障数据安全性以及提高数据计算效率，基于同态加密的站点位置需要从分布式数据库映射至区块链数据库，系统架构模型如图1(a)所示，从上至下依次分为应用层、存储层、网络与共识层、数据层和感知层。图1(b)是链上数据的存储结构，系统产生的交易记录会经过一系列哈希计算，最终以Merkle树这种数据结构进行链式存储，为了保证各节点间数据网络传输以及链上数据的容错和恢复，设计了传输网络与共识机制，通过链下存储链上维护的方式可以做到去中心化管理，因为智能合约是一个可根据触发条件来判断是否执行的程序[13]，将其部署在区块链上，既可以实现动态同城寄递路径规划、基于上下文加解密下一跳站点信息以及计算下一跳同城站点的功能，又可以让合约具备不可篡改的特点，提高了系统的可靠性。

在系统架构模型中，感知层用于获取保密文件的寄递信息，为系统提供数据保障，该层利用定位系统、传感器技术、射频识别技术(Radio frequency identification，RFID)、快速反应(Quick response，QR)码等技术收集实体的信息，包括车辆位置、车辆牌照、车辆到达时间和车辆图形数据等信息，为整体系统的完成打下良好基础。数据层分为感知数据和区块数据，感知数据从感知层中获取，经过处理后成为可识别的上下文数据，存入传统的分布式数据库中。基于同态加密的站点位置从链下数据库同步到链上后，经过哈希运算后得到的Hash值作为交易记录，再将交易记录加上时间戳并通过公钥进行数字签名，形成了区块数据，区块数据根据Merkle树这种数据结构进行链式存储，形成了区块链。在网络与共识层，感知数据通过由5G、物联网(Internet of things，IoT)形成的传输网络进行传输，实用拜占庭容错共识机制(Practical Byzantine fault tolerance，PBFT)保证着系统的容错和恢复，并确保所有区块节点的



(a) System architecture model　　(b) Storage structure of on-chain data

图1　系统架构模型

Fig.1　System architecture model

数据一致性[14]。存储层分为链上数据库和链下数据库;链下数据库为传统的分布式架构数据库,存储各自节点感知数据。对于站点而言,各站点数据库存储车辆进出站的具体信息以及保密文件寄递过程信息,包括车辆位置、车辆牌照、车辆到达时间和保密文件分拣状况等。对于车辆而言,链下数据库存储车辆接受任务、完成任务的时间节点以及任务信息。链上数据库为每个区块节点存储区块链数据,在链上记录交易信息以及智能合约的处理结果,如计算出的下一跳站点、寄递任务指派的车辆。链上数据和链下数据实时同步,利用链下存储链上维护的方式和分布式记账的手段可以做到去中心化管理。应用层服务于车辆与站点,利用部署在区块链上的智能合约提供了动态同城寄递路径规划、基于上下文加解密下一跳站点信息以及计算下一跳同城站点的功能,当车辆在规定时间到达规定站点,系统将自动调用合约实现相应的功能,最终实现数据的精准控制访问与隐私保护。

2　保密文件同城寄递自适应路径规划算法

保密文件同城寄递自适应路径规划算法包括基于区块链的动态同城寄递路径规划算法和基于上下文的加解密算法。其中,前者是一种根据贪婪法则运作的、在所有站点和终点位置被加密保护的情况下、动态实时寻找下一跳站点的路径规划算法,后者确保规划好的路径仅能被在正确时间到达正确位置的车辆获取。

2.1　基于区块链的动态同城寄递路径规划算法

在基于区块链的动态同城寄递路径规划算法中,各个站点的真实坐标都是被加密的。假设载有该保密文件的车辆此时到达站点S_i,其真实坐标为$(S_{i,x},S_{i,y})$,下一跳站点可能的选择有n个,分别为S_k,$k\in[0,n-1]$,真实坐标分别为$(S_{k,x},S_{k,y})$,$k\in[0,n-1]$,区块链的私钥为$s_k^{(h)}$,以上作为算法的输入。该算法的输出为下一跳站点S_{i+1},其坐标为$(S_{i+1,x},S_{i+1,y})$。定义$F()$为全同态加密函数,$F^{-1}()$为全同态解密函数。

$F()$加密的对象是明文转化成的布尔值序列。对明文的第i个布尔值加密时,首先选取不同的随机数q_i和$r_i(4r_i<s_k^{(h)})$,使用相同的$s_k^{(h)}$生成零密文的方式生成一系列公钥$p_{k_i}^{(h)}$,对每个布尔值加密使用不同的公钥$p_{k_i}^{(h)}$,其生成过程为

$$p_{k_i}^{(h)}=2r_i+s_k^{(h)}\cdot q_i \tag{2}$$

对明文第i个布尔值m_i加密,生成密文c_i的过程为

$$c_i=m_i+2r_i+p_{k_i}^{(h)}\cdot q_i \tag{3}$$

对于密文组成的长整数序列,通过模拟二进制补码,可以实现整数域的四则计算。$F^{-1}()$解密的对象是密文转化成的布尔值序列。对经过计算的密文的第i个布尔值c_i解密,还原明文m_i的过程为

$$m_i=(c_i \bmod s_k^{(h)}) \bmod 2 \tag{4}$$

(1) 各个站点在系统初始化阶段,将自身的位置S_k,$k\in[0,n-1]$坐标$(S_{k,x},S_{k,y})$,$k\in[0,n-1]$进行全同态加密为

$$\begin{cases}F(S_{k,x})\\F(S_{k,y})\end{cases}\quad k\in[0,n-1] \tag{5}$$

(2) 用户在提交寄递保密文件的申请时,对终点S_d坐标$(S_{d,x},S_{d,y})$进行全同态加密为

$$\begin{cases}F(S_{d,x})\\F(S_{d,y})\end{cases} \tag{6}$$

此外,如果保密文件同城寄递的过程中遇到转运站点状态发生变化、终点需要修改等情况需要重新规划路径,则重新加密新的站点或终点位置即可。派送路径不是提前规划及加密的,而是在可信的前提下可以在任何寄递阶段和位置实时进行修改优化的,这体现了本方案的实时动态性。

(3) 在正确时间到达正确站点的车辆触发智能合约,在每个可能的下一跳站点分别计算其坐标加密值($F(S_{k,x}),F(S_{k,y})$),$k\in[0,n-1]$与终点坐标加密值($F(S_{d,x}),F(S_{d,y})$)的加密近似距离$F(d_k)$为

$$F(d_k)=[F(S_{k,x})-F(S_{d,x})]^2+[F(S_{k,y})-F(S_{d,y})]^2 \quad k\in[0,n-1] \tag{7}$$

因为每个可能的站点都通过智能合约参与了加密距离的计算,因此不存在集中计算,实现了去中心化。这不仅减轻了单个服务器的计算开销,也保证了计算结果的可靠性,体现了本方案分布式计算的特点。

(4) 区块链使用自身私钥$s_k^{(h)}$解密$F(d_k)$,得到每个距离的明文d_k为

$$d_k=F^{-1}(F(d_k)) \quad k\in[0,n-1] \tag{8}$$

该近似距离的非减排列对应的站点与通过真实坐标计算得到的欧氏距离的非减排列对应的站点一致,因此,可以用于加密情况下度量两个站点间的距离。如果$d_k=0$,则说明当前站点就是最后一跳站点,终止运输。

(5) 区块链比较d_k,$k\in[0,n-1]$,寻找最小值,则最小值对应的站点就是下一跳站点S_{i+1},坐标为$(S_{i+1,x},S_{i+1,y})$。

(6) 车辆向下一跳站点S_{i+1}进行运输,此时S_{i+1}成为新的S_i,重复步骤(3)至步骤(6)。

由此,在没有任何一个实体获取终点真实坐标的情况下,区块链完成了动态同城寄递路径规划。计算得出的下一跳站点信息S_{i+1}通过基于上下文加密保护传送给车辆。

2.2 基于上下文属性的加解密算法

基于上下文的加解密算法保证了通过基于区块链的动态同城寄递路径规划算法计算得出的下一跳站点信息仅能被在正确时间到达正确位置的车辆获取。基于上下文的加解密算法是一种由发送者基于接收者属性参数进行加密、不会直接暴露接收者属性的一种安全通信算法。

加密算法的输入为待加密的明文(下一跳站点信息)S_{i+1}、接收者(车辆)的公钥p_k、接收者预期的属性参数向量$\boldsymbol{A}$,输出为密文(加密的下一跳站点信息)$C_{S_{i+1}}$和基于上下文加密的密钥C_K;解密算法的输入为$C_{S_{i+1}}$、C_K,以及接收者(车辆)的私钥s_k、接收者通过传感器实际采集到的属性参数向量$\boldsymbol{A}^{(m)}$,输出为明文(下一跳站点信息)S_{i+1}。区块链基于上下文加密和车辆基于上下文解密的具体步骤如下。

(1) 假设一接收者选择的属性参数有n个,则其预期的属性参数向量$\boldsymbol{A}$有n个维度,每个维度代表不同的属性参数为

$$\boldsymbol{A}=(a_0,a_1,\cdots,a_{n-1}) \tag{9}$$

定义$\boldsymbol{A}$中每个参数能接受的最大误差为$\boldsymbol{\omega}$为

$$\boldsymbol{\omega}=(\Delta a_0,\Delta a_1,\cdots,\Delta a_{n-1}) \tag{10}$$

合法的接收者预期的n维属性参数向量$\boldsymbol{A}_i$为

$$\boldsymbol{A}_i=(a_0+k_0\Delta a_0,a_1+k_1\Delta a_1,\cdots,a_{n-1}\pm k_n\Delta a_{n-1}) \tag{11}$$

式中$k_0,k_1,\cdots,k_{n-1}$为偏差系数,且$k_0,k_1,\cdots,k_{n-1}\in[-1,1]$。所有合法的接收者预期的$n$维属性参数向量构成$n$维子空间$\boldsymbol{S}$。

(2) 计算n维子空间$\boldsymbol{S}$各属性参数之和最小的点的向量$\boldsymbol{A}^{(L)}$为

$$\boldsymbol{A}^{(L)}=\begin{cases}a_0^{(L)}=a_0-\Delta a_0\\ a_1^{(L)}=a_1-\Delta a_1\\ \quad\vdots\\ a_{n-1}^{(L)}=a_{n-1}-\Delta a_{n-1}\end{cases}\tag{12}$$

计算接收区域内的补偿偏移向量$\boldsymbol{A}^{(o)}$为

$$\boldsymbol{A}^{(o)}=\begin{cases}a_0^{(o)}=a_0^{(L)}-2\Delta a_0\cdot\mathrm{floor}\left(\dfrac{a_0^{(L)}}{2\Delta a_0}\right)\\ a_1^{(o)}=a_1^{(L)}-2\Delta a_1\cdot\mathrm{floor}\left(\dfrac{a_1^{(L)}}{2\Delta a_1}\right)\\ \quad\vdots\\ a_{n-1}^{(o)}=a_{n-1}^{(L)}-2\Delta a_{n-1}\cdot\mathrm{floor}\left(\dfrac{a_{n-1}^{(L)}}{2\Delta a_{n-1}}\right)\end{cases}\tag{13}$$

式中floor()为向下取整函数。接着,构造$n-1$个映射为

$$F(\boldsymbol{A})=\begin{cases}f_0(a_0)=2\Delta a_0\cdot\mathrm{floor}\left(\dfrac{a_0-a_0^{(o)}}{2\Delta a_0}\right)+a_0^{(o)}\\ f_1(a_1)=2\Delta a_1\cdot\mathrm{floor}\left(\dfrac{a_1-a_1^{(o)}}{2\Delta a_1}\right)+a_1^{(o)}\\ \quad\vdots\\ f_{n-1}(a_{n-1})=2\Delta a_{n-1}\cdot\mathrm{floor}\left(\dfrac{a_{n-1}-a_{n-1}^{(o)}}{2\Delta a_{n-1}}\right)+a_{n-1}^{(o)}\end{cases}\tag{14}$$

(3) 生成随机密钥K,并使用K对称加密S_{i+1},得到$C_{S_{i+1}}$。

(4) 将随机密钥K与步骤(2)中对接收属性参数向量$\boldsymbol{A}$进行映射后所得的结果$(f_0(c_0),f_1(c_1),\cdots,f_{n-1}(c_{n-1}))$进行异或,得到临时密钥$K_v$。

(5) 使用接收者(车辆)的公钥p_k非对称加密K_v,得到基于上下文加密的密钥C_K。

(6) 假设接收者通过传感器实际采集到的n维属性参数向量$\boldsymbol{A}^{(m)}$为

$$\boldsymbol{A}^{(m)}=(a_0^{(m)},a_1^{(m)},\cdots,a_{n-1}^{(m)})\tag{15}$$

(7) 接收者(车辆)使用其私钥s_k非对称解密C_K,得到临时密钥K_v。

(8) 对$\boldsymbol{A}^{(m)}$进行映射处理,有

$$F(\boldsymbol{A}^{(m)})=(f_0(a_0^{(m)}),f_1(a_1^{(m)}),\cdots,f_{n-1}(a_{n-1}^{(m)}))\tag{16}$$

式中如果$\boldsymbol{A}^{(m)}\in\boldsymbol{S}$,也就是$\boldsymbol{A}^{(m)}$满足式(17)。

$$\begin{cases}\left|a_0^{(m)}-a_0\right|\leqslant\Delta a_0\\ \left|a_1^{(m)}-a_1\right|\leqslant\Delta a_1\\ \quad\vdots\\ \left|a_{n-1}^{(m)}-a_{n-1}\right|\leqslant\Delta a_{n-1}\end{cases}\tag{17}$$

则$F(\boldsymbol{A}^{(m)})=F(\boldsymbol{A})=(a_0^{(o)},a_1^{(o)},\cdots,a_{n-1}^{(o)})$。

(9) 将$\boldsymbol{A}^{(m)}$的映射结果$(f_0(a_0^{(m)}),f_1(a_1^{(m)}),\cdots,f_{n-1}(a_{n-1}^{(m)}))$与$K_v$进行异或,还原随机密钥$K$。

(10) 使用K对称解密$C_{S_{i+1}}$,得到S_{i+1}。

由区块链进行基于上下文加密保护下一跳站点信息、车辆基于上下文解密获取下一跳站点信息的过程如图2所示。

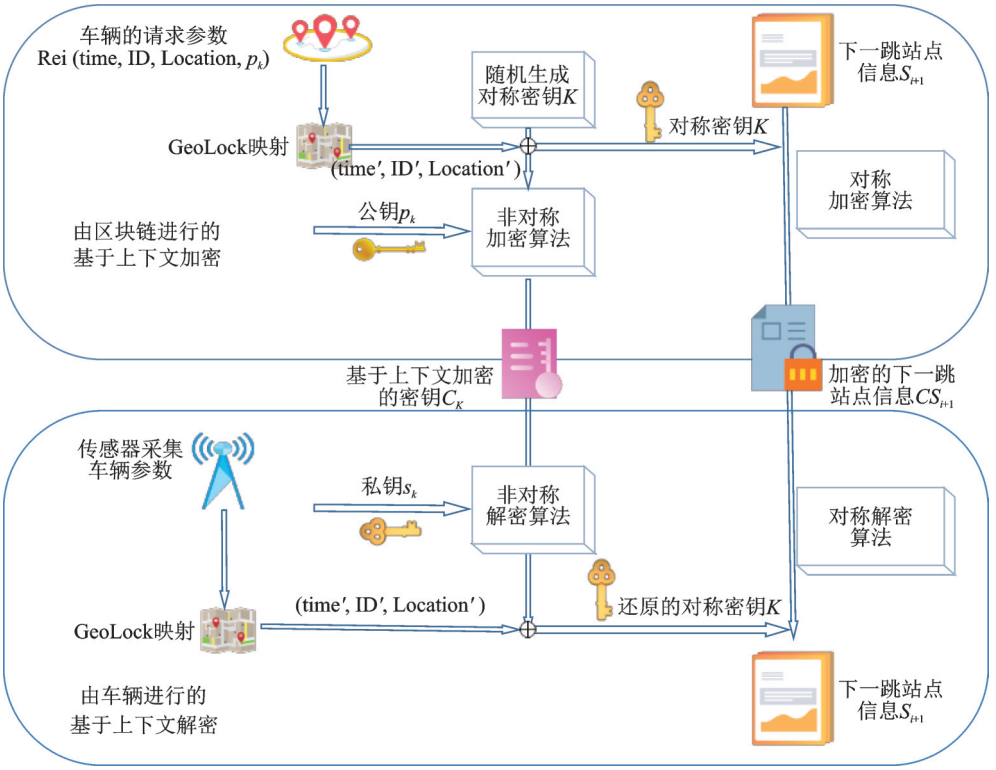


图2 基于上下文加密解密的流程图

Fig.2 Flow chart of context-based encryption and decryption

3 系统实现与测试

本文实现了区块链的保密文件南京同城寄递系统[15]，并对基于区块链的保密文件同城寄递自适应路径规划算法进行了测试。实验模拟终点位置、各个站点位置被加密保护的情况下车辆提交请求、触发区块链调用智能合约动态规划路径、获取下一跳站点的过程。

智能合约同态计算结果分析在后端控制台，部署在区块链上的智能合约能够计算处理加密过的站点位置数据，在合理的时间内得出下一跳站点位置，通过基于上下文加密后返回给车辆，实现同城配送路径的实时动态规划。

不同属性个数n(即式(9～17)中各向量的维数n)对路径规划计算代价影响测试：对车辆进行同城寄递的场景进行仿真，假设车辆用于密钥生成、加密和解密的属性参数个数n从1增至10个，属性参数可以选择经度、纬度、海拔、ID、时间戳、速度和方位角等能唯一标识可信车辆的参数，实验结果如表1所示。

结果显示，属性参数个数n从1增至10个的过程中，密钥生成时间没有明显变化，加密、解密时间略有增加，但都在合理的范围内。在本方案中，结合同城寄递的实际场景，车辆选择4个属性，即n取4，分别为经度、纬度、ID和时间戳，因此计算代价可以接受。

不同站点个数对路径规划计算处理时间影响测试：对车辆进行同城配送的场景进行仿真，将车辆

的属性参数个数设置为4,探究邻居站点个数的增加对于智能合约进行的全同态加密路径规划时间有无不可接受的影响,测试结果如表2所示。

表1　不同属性个数对计算代价影响

Table 1　Effect of different numbers of attributes on calculation cost

属性个数n	密钥生成时间/ms	加密时间/ms	解密时间/ms
1	15	170	64
2	14	174	71
3	15	176	72
4	14	179	104
5	16	183	110
6	16	185	113
7	15	191	115
8	17	196	121
9	16	199	128
10	17	203	135

表2　不同站点个数对路径规划计算处理时间影响

Table 2　Effect of the number of different stations on processing time of route planning calculation

邻居站点个数	路径规划时间/ms	邻居站点个数	路径规划时间/ms
1	2 144	11	2 539
2	2 186	12	2 582
3	2 212	13	2 628
4	2 265	14	2 664
5	2 290	15	2 735
6	2 321	16	2 780
7	2 370	17	2 867
8	2 412	18	2 940
9	2 450	19	3 050
10	2 492	20	3 172

结果显示,随着站点个数的增加,路径规划的时间从2 144 ms开始近似指数上升,但是一般可能选择的下一跳站点个数不会超过20个,因此路径规划时间均在可以接受的范围内。

4　结束语

针对同城道路复杂保密文件寄递效率低和隐私泄露问题,本文基于区块链、全同态加密以及上下文加密等技术,提出了一种基于区块链的保密文件同城寄递自适应路径规划算法,解决保密文件的同城寄递问题。系统利用区块链的共识机制和智能合约算法,各分布式节点通过同态加密计算构成。车辆利用自身上下文信息才可以加解密下一条站点信息,具有防冒充的功能,也解决了车辆、站点和快递员之间互不信任的问题,提高了同城寄递背景下保密文件的配送效率与安全性。

另外,本文对全系统模块方案、整体流程以及原型系统的实现,分析了智能合约同态计算结果,针对不同属性个数、不同站点个数对路径规划计算代价影响进行了测试,测试结果表明保密文件同城寄递系统中的路径规划算法具备机密性、完整性和防篡改的功能,该技术为解决保密文件的及时寄递应用中的隐私泄露问题提供了有力的应用技术支撑。

参考文献:

[1]　全国人民代表大会常务委员会. 中华人民共和国保守国家秘密法[Z]. 北京: [s.n.], 2010-04-29.
Standing Committee of the National People's Congress. Law of the peoples republic of China on guarding state secrets[Z]. Beijing: [s.n.], 2010-04-29.

[2]　肖亮,李强达,刘金亮. 云存储安全技术研究进展综述[J]. 数据采集与处理, 2016, 31(3): 464-472.
XIAO Liang, LI Qiangda, LIU Jinliang. Survey on secure cloud storage[J]. Journal of Data Acquisition and Processing, 2016, 31(3): 464-472.

[3]　RIVEST R L, ADLEMAN L M, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Compuation, 1978, 4(11): 169-179.

[4] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[5] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of International Conference on the Theory and Application of Cryptographic Techniques. Prague, Czech: [s.n.], 1999: 223-238.

[6] GENTRY G. Fully homomorphic encryption using ideal lattices[J].Proceedings of the Annual ACM Symposium on Theory of Computing, 2009, 9(4): 169-178.

[7] NACCACHE S. A new public key cryptosystem based on higher residues[C]//Proceedings of the 5th ACM Conference on Computer and Communications Security. New York: ACM, 1998: 59-66.

[8] DIJK M, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[C]//Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: [s.n.], 2010: 24-43.

[9] REGEV O. New lattice-based cryptographic conctructions[J]. Journal of the ACM, 2004, 51(6): 899-942.

[10] 周倩,秦小麟,丁有伟. 无线传感器网络中基于哈希函数的上下文隐私保护[J]. 南京理工大学学报(自然科学版),2017,41(6): 753-759.
ZHOU Qian, QIN Xiaolin, DING Youwei. Hash-based contextual privacy preservation in wireless sensor networks[J]. Journal of Nanjing University of Science and Technology, 2017, 41(6): 753-759.

[11] 周倩,秦小麟,丁有伟. 基于攻击感知的能量高效源位置隐私保护算法[J]. 通信学报,2018,39(1): 101-116.
ZHOU Qian, QIN Xiaolin, DING Youwei. Preserving source-location privacy efficiently based on attack-perceiving in wireless sensor network[J]. Journal on Communications, 2018, 39(1): 101-116.

[12] 陈兵,成翔,张佳乐,等.联邦学习安全与隐私保护综述[J].南京航空航天大学学报, 2020,52(5): 675-684.
CHEN Bing, CHENG Xiang, ZHANG Jiale, et al. Survey of security and privacy in federated learning[J].Journal of Nanjing University of Aeronautics & Astronautics,2020,52(5): 675-684.

[13] 林诗意,张磊,刘德胜.基于区块链智能合约的应用研究综述[J].计算机应用研究,2021,38(9): 2570-2581.
LIN Shiyi, ZHANG Lei, LIU Desheng. Survey of application research based on blockchain-smart-contract[J].Application Research of Computers,2021,38(9): 2570-2581.

[14] HU Wei, HU Yawei, YAO Wenhui, et al. A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles[J]. Special Section on Big Data Technology and Applications in Intelligent Transportation, 2019(99): 1.

[15] 周倩,张添龙,吴加洋,等. 一种基于区块链的快递上下文位置隐私保护方法: CN202111398742.0[P]. 2022-03-18.
ZHOU Qian, ZHANG Tianlong, WU Jiayang, et al. A blockchain based privacy protection method for express context location: CN114201764A[P]. 2022-03-18.

作者简介:

周倩(1983-),**通信作者**,女,讲师,博士,硕士生导师,研究方向:密码应用技术、网络安全、隐私保护、物联网,E-mail:zhouqian@njupt.edu.cn。

张添龙(2000-),男,本硕连读生,研究方向:区块链、分布式系统。

吴加洋(2001-),男,本科生,研究方向:区块链、网络安全。

韩忠旭(2001-),男,本硕连读生,研究方向:区块链、人工智能。

戴华(1982-),男,教授,博士生导师,研究方向:区块链、隐私保护、物联网。

(编辑:陈珺)