刘宇琛,张留学. 可搜索加密技术在金融交易行为中的应用[J]. 湖南科技大学学报(自然科学版), 2024, 39(3):116-124. doi:10.13582/j.cnki.1672-9102.2024.03.015

LIU Y C, ZHANG L X. Application Research of Searchable Encryption Technology into Financial Transaction Behaviors [J]. Journal of Hunan University of Science and Technology (Natural Science Edition), 2024, 39(3):116-124. doi:10.13582/j.cnki.1672-9102.2024.03.015

可搜索加密技术在金融交易行为中的应用

刘宇琛[1],张留学[2*]

(1.长沙理工大学 经济与管理学院,湖南 长沙 410114; 2.长沙泥娃数字科技有限公司,湖南 长沙 410005)

摘 要:针对金融交易行为信息管理的安全问题,基于同态加密算法的原理,研究了分离码编解码、路径散列消息摘要和语义树索引算法.在此基础上,利用分离码编解码算法作为同态加密的加解密手段,结合路径散列消息摘要算法、语义树索引算法,构建金融交易行为信息的安全存储方法及密文搜索系统.结果表明:利用分离码分组编码算法将信息转换为变换序列和位数序列,可以实现用密文建立全文检索;通过信息分组、路径散列计算、结果序列调和散列,结合输出字符串的设定,提出不可逆消息摘要的生成方法;基于语句的索引算法,采用密文搜索和原来语句搜索的一致性原则,构建密文搜索系统;构建的全文暨密文检索系统,可以实现密文的快速、安全检索,能够保证用户交易行为的数据、隐私、计算和分析的安全.

关键词:金融交易行为;可搜索加密;分离编解码;密文检索;语义树搜索

中图分类号:TP393.08 **文献标志码**:A **文章编号**:1672-9102(2024)03-0116-09

Application of Searchable Encryption Technology into Financial Transaction Behaviors

LIU Yuchen[1], ZHANG Liuxue[2]

(1. School of Economics and Management, Changsha University of Science and Technology, Changsha 410114, China;
2. Changsha Niwa Digital Technology Co., Ltd., Changsha 410005, China)

Abstract: Addressing the security issues in the information management of financial transaction behaviors, this paper investigates the Separating Codec, Path Hash Message Digest, and Semantic Tree Indexing Algorithms based on the principles of Homomorphic Encryption Algorithms. Building upon this research, the Separating Codec Algorithm is employed as the encryption and decryption method for homomorphic encryption, integrated with the Path Hash Message Digest algorithm and Semantic Tree Indexing algorithm, to construct a secure storage method and ciphertext search system for financial transaction behavior information. Results indicate that by utilizing a Separating Codec Block Coding Algorithm to convert information into a transformation sequence and a bit sequence, it is feasible to establish a full-text search capability by using ciphertexts. Furthermore, an irreversible message digest generation method is proposed through information grouping, path hashing computation, result sequence modulation and hashing, in conjunction with the setting of output strings. Based on the sentence-level indexing algorithm, a ciphertext search system is constructed by adopting the consistency principle between ciphertext search and original sentence search. The constructed full-text and ciphertext retrieval system can achieve fast and secure retrieval of ciphertexts, ensuring the security of user transaction data,

收稿日期:2024-03-14

* **通信作者**,E-mail: zhangliuxue@126.com

privacy, computation, and analysis.

Keywords: financial transaction behavior; searchable encryption; separate encoding and decoding; ciphertext retrieval; semantic tree search

信息安全一直是金融交易关注的热点和难题[1-2].近年来,随着计算机技术、网络技术和通信技术的高速发展,金融交易行为过程需将大量私密数据,如客户个人资料、统计报表和交易信息等数据迁移到云端服务器,一旦这些重要的信息泄露,将会造成不可估量的损失和严重社会危害[3-4].实现金融交易行为数据在传输、存储、搜索和计算过程中的信息安全,对金融数字化具有重要研究价值.

当前,为了保证数据安全和用户隐私,大多通过加密方式将数据以密文形式存储[5-6].如果简单地采用传统加密方法,一旦数据被加密,则无法对其进行任何操作,除非拥有正确的密钥,这将大大限制了加密数据的使用价值[7-8].可搜索加密技术则打破了这一限制,该技术可以在不暴露明文的情况下,将数据进行加密后存储到云端服务器,实现对密文进行检索,用户只需要对返回的文件进行解密,使得加密数据在保持隐私的同时,也能实现高效的检索[9-10].因此,学者们对可搜索加密技术的原理、算法、模型以及数据集进行了广泛研究,在信息安全存储和搜索方面取得了较丰硕的成果[11-13].尽管人们在研究和推广可加密技术上取得了长足进步,但大多数机制仍存在不同程度的额外信息泄露,容易被攻击者捕获用于恢复明文信息与查询条件,强化金融交易行为密文检索中的隐私保护特性仍需深入系统研究[14].此外,当前可搜索加密系统的全文搜索和信息加解密技术主要采用倒排序表的方式,系统在查询过程需要对关键词进行全文重复对比,造成搜索体积和搜索计算指数增加,特别是金融交易行为存储了客户海量私密信息,若继续采用传统的密文搜索方式,势必会导致系统索引不可计算[15-16].然而,如何高效、安全地检索金融交易行为的非结构化数据,仍是一个亟待解决的难题.

为此,本文从金融交易安全和搜索效率的实际需求出发,系统研究分离码编解码、路径散列消息摘要和语义树索引算法,利用分离码编解码算法作为同态加密的加解密手段,结合路径散列消息摘要算法,语义树构建全文暨密文检索系统,实现金融交易行为信息的密文快速和安全搜索,研究成果将有效地推动可搜索加密在金融交易行为中的应用和推广.

1　同态算法原理及密文搜索架构

1.1　同态算法原理

同态加密(Homomorphic Encryption, HE)是指满足密文同态运算性质的加密算法,即数据经过同态加密之后,对密文进行特定的计算,得到的密文计算结果在进行对应的同态解密后的明文,等同于对明文数据直接进行相同的计算.常见的同态加密运算有

加法同态:$f(A)+f(B)=f(A+B)f(A)+f(B)=f(A+B)$;

乘法同态:$f(A)\times f(B)=f(A\times B)f(A)\times f(B)=f(A\times B)$.

全同态加密:支持对密文进行任意形式的计算(即满足加法和乘法).全同态加密方案的一般结构:

密钥生成:对于给定的环 R 和理想 I 的基 B_I, $\mathrm{IdealGen}(R,B_I)=(B_J^{\mathrm{sk}},B_J^{\mathrm{pk}})$ 满足 $I+J=R$,其中 $B_J^{\mathrm{sk}},B_J^{\mathrm{pk}}$ 为理想 J 的基 B_J 组成的私钥和公钥.

加密:选择随机向量 $\boldsymbol{r},\boldsymbol{g}$,消息 $m\in\{0,1\}$,生成密文 $\mathrm{ct}=\mathrm{Enc}(m)=m+\boldsymbol{r}\cdot Br+\boldsymbol{g}\cdot B_k$

解密: $\mathrm{Dec}(\mathrm{ct},B_J^{\mathrm{sk}})=(\mathrm{ct}-B_J^{\mathrm{sk}}\cdot(B_J^{\mathrm{sk}})^{-1}\times\mathrm{ct})\bmod B_I$

密文加法: $\mathrm{ct}_1+\mathrm{ct}_2=\mathrm{Enc}(m_1)+\mathrm{Enc}(m_2)=m_1+m_2+(r_1+r_2)B_I+(g_1+g_2)B_J^{\mathrm{pk}}$

密文乘法:

$$\mathrm{ct}_1\mathrm{ct}_2=\mathrm{Enc}(m_1)\mathrm{Enc}(m_2)=$$

$$m_1m_2+(m_1r_2+m_2r_1+r_1r_2B_I)B_I+(m_1g_2+m_2g_1+g_1g_2B_J^{\mathrm{pk}})B_J^{\mathrm{pk}}+(r_1g_2+r_2g_1)B_IB_J^{\mathrm{pk}}$$

1.2　密文搜索架构

本文实现密文全文检索参照同态加密的原理构建:

1)分离编解码算法:FlEnc 为加密算法,FLDec 为解密算法;

密钥:0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-

明文:分离编解码的方法

对应密文:BzExD3 CKXVY2 my+Fz2 D3qwD3 qiEVm2 Vq+Il2

明文:分离编解码的方法和系统

对应密文:BzExD3 CKXVY2 my+Fz2 D3qwD3 qiEVm2 Vq+Il2 Bb9zD3 PKXVX2 v2

从上可以得出,明文和密文具备前缀的一致性.

2)语义树索引算法假定为 YTree($\{w_0,w_1,\cdots,w_{n-1}\}$)= $\{T_0,T_1,\cdots,T_{m-1}\}$:

由增量 Hash 算法构建,假定语句含有文字序列为$\{w_0,w_1,\cdots,w_{n-1}\}$,则特征码计算如下:

对应序列为$\{T_0,T_1,\cdots,T_{m-1}\}$,其中 T_i=hash($T_{i-1}+w_{i-1}$),当 i=0 时,T_0=hash(w_0).

3)同态算法构建,经过分离编解码的文字序列和原文存在前缀一致性的对应关系,即经过语义树索引构建的全文搜索,提供基于密文的全文检索,满足同态计算的要求:

假定密钥为 K,编码算法为 FlEnc($\{w_0,w_1,\cdots,w_{n-1}\},K$)=$\{F_0,F_1,\cdots,F_{m-1}\}$,文字序列加密后为$\{F_0,F_1,\cdots,F_{m-1}\}$;

对应语义树 YTree($\{F_0,F_1,\cdots,F_{m-1}\}$)=$\{Ft_0,Ft_1,..,Ft_{m-1}\}$;

语义树序列$\{T_0,T_1,\cdots,T_{m-1}\}$和$\{F_{t0},F_{t1},\cdots,Ft_{m-1}\}$存在一定的对应关系,这点由分离编解码的特性决定;

因而查询 T_0,T_1,T_3组合对应于 F_{t0},F_{t1} 以及后续的组合.

查询“分离编解码”对应“BzExD3 CKXVY2 my+Fz2 D3qw”,从而可以在密文建立的语义树索引中查到.

2 分离编解码算法

利用数学不同进制之间的转换,结合变换的码表,实现信息编解码,采用码表定义的特性和进制转换,对明文进行计算,把码表等同为密码进行信息编解码,主要包括设计分离码表、信息编码和信息解码.

2.1 设计分离码表

基于分离码表,利用分离码分组编码算法将信息转换为变换序列和位数序列,实现信息编码,信息编解码流程见图 1.通过给定进制的基本字符表示分离码表,默认分离码表进制为 62 进制、读取信息的基本单位为 64 位,字典字符由 0~9 数字、英文字母大写 A~Z 和小写 a~z 共 62 个字符,分别表示 0~61 的数,即 62 进制的基本数字.

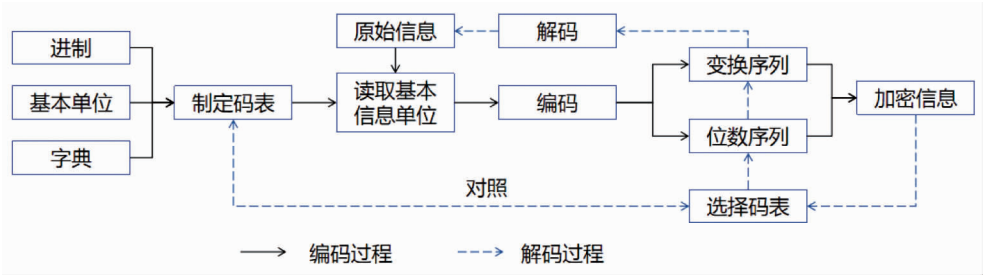

图 1 编解码流程

2.2 信息编码

信息编码根据分离码表“读取信息基本单位”的要求,读取指定位数信息赋值给整数,然后根据转换的要求转换成分离码表定义的进制,转换的结果字符串记录到变换序列,转换后的结果字符串的长度记录到位数序列,一直持续到字符转化完毕.

2.3 信息解码

将从位数序列中读取位数信息,从变换序列中按位数读取相关的字符串,查找分离码表字典变换成相

应的数字,结合分离码表定义转换的进制,转换为整数,存入到文件中,一直到转换完毕,得到相关的文件,即完成信息解码.

3　基于路径散列的消息摘要算法

基于路径散列的消息摘要方法和系统的实现,主要通过信息分组、路径散列计算、结果序列调和散列,结合输出字符串的设定,从而输出的消息摘要.

3.1　信息分组

将消息摘要用数组 $S[i]$ 描述,i 从 0 到 2^k-1.假定信息分组的 bit 数定义 k,则有 $S[i]$ 的值小于 2 的 2^k-1.变换序列的大小等于消息摘要的大小,单元值为 0 到 2^k-1.对消息按 bit 位进行分组.计算机输入的字符最小单元为字符型,字符型占位为 8 个 bit,假定摘要存储单元的大小为 k 个 bit,则分组规则如下:分组数为 h,选取的字符个数为 g,则有 $8g=hk$.分组每次选取 g 个字符,分组后产生 h 个 kbit 的单元;分组序列定义为 $D_i[h]$,i 表示输入序列的第 i 个分组.假定分组的数组为 $D_i[j]$,其中 j 为 0 到 $h-1$,对分组数组进行散列计算.计算步骤如下:循环从 0 到 $h-1$;一次散列计算,散列计算按路径选择策略结合散列算法实施.路径规划:假定变换序列为 R,k 为分组信息的位数,R 含有 $2k$ 个单元,元素取值范围为 0 到 2^k-1;循环设定:设定循环的次数,假定为 p 次,p 为路径深度;分组散列计算.分组信息 $D_i[h]$,对 h 进行循环运算.

3.2　路径散列计算

对分组信息散列,分组信息 $D_i[h]$,对 h 进行循环运算;计算单元来自消息摘要序列 $S[i]$,分组信息 $D_i[h]$,假定路径选择为一元路径选择,即 $F(i+1)=R[F(i)]$;分组信息再散列,计算单元来自消息摘要序列,变换序列,假定路径选择为二元路径选择,即 $Rf(i+1,Di+1[h])=R[F(i),Di[h]]$;假定算法为 $H(S[i],Di[h])$,则有 $S[i]=H(S[i],Di[h])$,h 为分组信息的大小;分组散列算法表示如下:按路径算法选择参与计算的值 $S[F(i)]$,$Di[h]$,假定路径函数为 $F(i)$,路径深度为 p,算法为 $H(S[i],Di[h])$,则下列计算循环 p 次;$Pt=F(i)$,$S[Pt]=H(S[Pt],D_i[h])$.选择下一步路径,$F(i+1)=R[F(i)]$,即 $Pt=F(i+1)=R[F(i)]$.

重复上一步计算,直到满足循环条件即可;再散列,按路径算法选择参与计算的值 $S[Pt]$,假定 Rf 为 i 和 $D_i[h]$ 的二元路径选择函数,路径深度为 p,算法为 $H(S[i],R[i])$,则下列计算循环 p 次:$Pt=Rf(i,D_i[h])$,$S[Pt]=H(S[Pt],R[i])$.选择下一步路径,即 $Pt=R[Pt]$,重复上一步计算,直到满足循环条件即可.

3.3　结果序列调和散列

结果序列调和散列是对消息摘要序列的值按路径散列的算法进行计算,所述结果序列调和散列运算单元为消息摘要序列中的值,假定路径选择为一元路径选择算法 $F(i)$,计算方法定义 $H(O[i],S[Pt])$,具体描述如下:

定义输出序列为 $O[i]$,大小等于摘要序列的大小,摘要序列为 $S[i]$,则有调和计算单元为 $S[i]$,$O[i]$;赋初值,$O[i]=S[i]$;计算路径选择,定义计算路径深度为 p,则循环 p 次:路径选取 $Pt=F(i)$;$O[i]=H(O[i],S[Pt])$;选择下一步路径,即 $Pt=R[Pt]$,重复上一步计算,直到满足循环条件即可;把 $O[i]$ 复制到 $S[i]$;消息摘要序列为 $S[i]$.

4　语义树索引算法

语义树索引技术主要根据语句中文字的排列顺序,计算文字对应语句的特征编码,利用链式存储技术,实现对应语义树.形象地描述:文字为语义树上的基本节点,语句为语义树的枝条,所有的枝条结合在一起构建语义树.语义树上的分枝具有同样的根节点文字.

语义树的索引技术指的是在语义树上查找语句,通过语句找到对应文档的过程.一般来说语义树的索引包括:

1)语义树.利用语句中文字的特征码,结合该文字前面的特征码组建.主要技术为特征码和链式存储.

2)语句和文档的关系.主要存储语句特征码和文档关系.

通过最大匹配语句找到文档的过程,称为语义树的索引.

语义树索引技术主要采用的技术:

1)特征编码技术.主要由增量 Hash 算法构建,假定语句含有文字序列为$\{w_0,w_1,\cdots,w_{n-1}\}$,则特征码计算为 $T_i=\text{hash}(T_{i-1}+w_{i-1})$,当 $i=0$ 时,$T_0=\text{hash}(w_0)$.

2)链式存储技术.语义树的存储单元为$\{T_i,w_i,T_{i-1},f\}$,其中 f 表示是否为句尾.

3)语句和文档的关系.主要存储具有句尾标识的特征码和文档 ID 的关系.

4)语句匹配查询技术.分为两种方式:计算语句的特征码,在语义树中查找,去找到最大深度的特征码,然后在语义树中匹配语句,根据语句找到文档.在语义树中找到第一个文字对应的记录集合,从集合中取出特征码,结合查询的语句,去掉第一个字符,和后续的文字计算特征码,在语义树中查找,去找到的最大深度的特征码,然后在语义树中匹配语句,根据语句找到文档.

4.1 序列特征信息表示方法

文档信息内容文字排列如为 $w_0w_1w_{2\cdots}w_{n-1}$,依次表示为文字 1 到文字 n 的排列;通过对文字信息的增量 Hash 编码,w_0 的特征序列定义为 t_0,$t_0=\text{hash}(w_0)$;w_1 的特征序列定义为 t_1,$t_1=\text{hash}(t_0+w_1)$;以此类推,w_{n-1}的特征序列定义为 t_{n-1},$t_{n-1}=\text{hash}(t_{n-2}+w_{n-1})$;$t_i$ 其中 $i=0,1,2,\cdots,n-1$ 表示该语句的语义特征序列.

4.2 语义树构建

基于文字的表示习惯,以语句为单位构建文字和文字之间的前后关系,具体表现为存储的内容包括:前文字的特征信息编码,当前文字信息,当前文字序列的特征信息编码;语义树基本构建单元包括:$\{t_{i-1},w_i,t_i,\text{flag}\}$,其中 flag 为该特征在句子中位置的标识(居首、句中和句尾),由此组建语义树;基于文字的编码规定,结合文字特有的分割符对语句进行切分,对语句进行特征序列的编码处理.基于文字的编码规定实现单一语种、多语种结合的语义树.通过对组建语义树的编码范围的给定,可以构建单一语种、多语种组合甚至于不分语种的语义树.

4.3 特征序列查找

通过构建查找内容的特征序列,在特征语义树中查找该记录,特征序列的最大化查找,首先查找位于句尾的特征序列,找到进行关联文档的查询即可;否则进入特征序列的递减查找;特征序列的递减查找,从句尾特征序列向前递减查找,以此递归直到找到特征序列或者没有找到句首的特征序列为止;查找到的语义特征序列如果位于文档尾部,则可以从语义特征序列和文档的关联存储查找文档标识,通过文档标识进行文档的查找;否则进入查找句尾特征序列;在语义树中查找句尾特征序列:语义树基本存储结构为$\{t_{i-1},w_i,t_i,\text{flag}\}$,查找 t_{i-1}特征序列,通过语义树首先找到 t_i,判断是否为句尾,如果是,则从文档和特征序列的关系表中查询文档的标识,如果否,则继续查找,直到找到句尾特征序列,根据特征序列查询文档标识.

5 密文搜索方法

密文检索利用分离编解码技术产生的密文建立索引,文档的存储可以采用用户自定义安全加密方式的密文,查询采用分离码加密的密文,查询的结果为加密的密文,从而实现从建立检索阶段、存储阶段、传输阶段和计算阶段的全程安全机制.构建密文检索系统过程如下:

假定明文为 $w_0\ w_1\cdots w_{n-1}$,对应语义树编码 $\text{ew}_0\ \text{ew}_1\cdots\text{ew}_{n-1}$;

假定分离编解码算法,密钥为 k,编码函数为 $\text{flencode}(w_0w_1\ w_2\cdots w_{n-1},K)=\{\ \text{flew}_0\ \text{flew}_1\cdots\text{flew}_{m-1}\}$;

解码函数为 $\text{flDec}(\text{fw}_0\ \text{fw}_1\cdots\text{fw}_{m-1},k)=\ w_0\ w_1\cdots w_{n-1}$;

$\text{fw}_0\ \text{fw}_1\cdots\text{fw}_{m-1}$对应语义树编码 $\text{mew}_0\ \text{mew}_1\cdots\text{mew}_{m-1}$;

存在基于密文的 $\text{ew}_0\ \text{ew}_1\cdots\text{ew}_{n-1}$查询对应基于密文的 $\text{mew}_0\ \text{mew}_1\cdots\text{mew}_{m-1}$的结果.

密钥:0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-.

明文:分离编解码的方法,对应密文:BzExD3 CKXVY2 my+Fz2 D3qwD3 qiEVm2 Vq+Il2.

明文:分离编解码的方法和系统,对应密文:BzExD3 CKXVY2 my+Fz2 D3qwD3 qiEVm2 Vq+Il2 Bb9zD3

PKXVX2 v2.

分离码算法特点:采用码表定义的特性和进制转换,对明文进行计算,把码表等同为密码,特点是计算的结果和原文具备一定程度的前缀一致性.

语义树索引特性:采用前缀最大匹配语句的形式编码查询;分离码的特性最大限度满足语义树索引特性,于是存在可解密搜索.

密文检索示例:

明文:分离编解码的方法和系统

密钥:0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-

密文:BzExD3 CKXVY2 my+Fz2 D3qwD3 qiEVm2 Vq+Il2 Bb9zD3 PKXVX2 v2

语义树编码,根据要求可以截取长度,实际中采用 24 个字符即可满足要求,截取后的字符为存储数据,在此基础上建立索引:

U8KOt=KBeK6aLWExgbSdVoy=mAxSoBQy2Yh53JYnne=BI7TqfOYieHiqFx0YPcG4RA0sGJTGU6CmzuEmA3FoLVvYKpJNbI6hf7q-SvqsT1EIBQmKXTCqCWkNxbmZ-3k8ekblap0hH7-ppZ6e76LxgYirwM4I=ykEQ7mAd2uq4OGtXqVSuv3-dJS9KP=hqBmVxRMmrQv8DSBDknK7WRRP6r1PrbVWCEGJBYh26SYdfxqvYebKUnn25JWQXkQ7rq61FvqL5rp2kNANXKPSIQDaZ492QulaVUOYO3MU-vA9i-ybClx9bNFlqxvte-MZmveykt9Kq4pjk2vL64v4EKZyOisHPb9wZMDv5wpkVIRpuF88ZrvqcdyUkewq33iPa6QEzpKiFX9U4d-y5hkfxOZk=1rUPq0XKJ-vDP9f7yrp0ZwZFhyNV5MUh4qcZxkuq-cBOHI4cNC-3qba7GVf8y4dGW0L0wNI=285o55EPbY9DbW-4JNYNaVnEZsUfBA7NQCNw16s-limZ8-UjUCD4SoccbfiaJbt40eIOFTCJ7j=zxqIOn

最后一个编码为句尾编码,与加密文本关联.

6　可搜索加密在金融交易行为中的应用

在金融交易行为中,有大量记录性的日志文档和交易数据,利用分离编解码算法对日志文档进行加密,通过信息分组、路径散列计算、结果序列调和散列,生成不可逆的消息摘要,基于语句的索引算法,采用密文搜索和原来语句搜索的一致性原则,构建密文搜索系统,在此基础上实现金融交易信息的可加密搜索,示例如下所示.

6.1　建立密文索引

假定密钥:总 2 大薄 i 最理能轻编视 d 性 46m9 件器系志可度本戴 c 全语列算升型文言 3 力龙码速 sa 锐运 0 处玲尔 1 四至战提模珑行第压达频月缩 p 代高 8

系统信息录入界面见图 2.

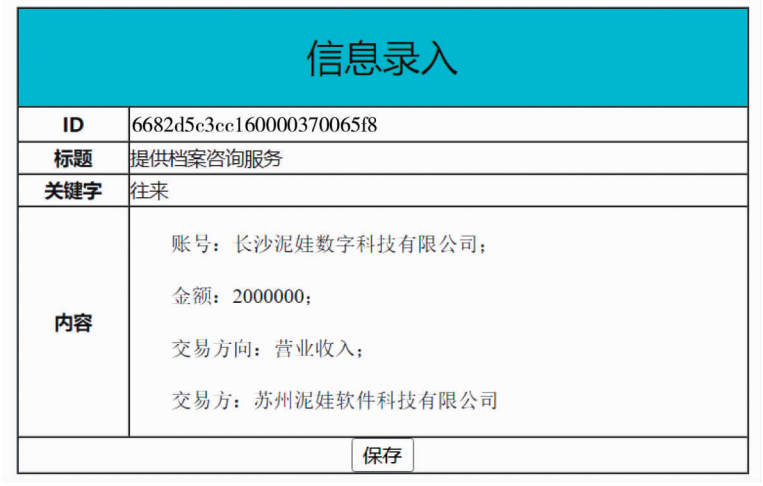

图 2　信息录入界面

明文数据如下:

{

"title_s":"账号往来",

"content":"账号:长沙泥娃数字科技有限公司;

金额:2000000;

交易方向:营业收入;

交易方:苏州泥娃软件科技有限公司",

"answer":"提供档案咨询服务",

"_id": "6682d5c3cc160000370065f8"

}

加密后传输到服务器,服务器由此建立索引,数据如下:

[{"title_s":"达缩 1 锐可薄 件大视",

"content":"达珑玲行志薄 0 行戴码 1 大 运运 6i 战大 提 8 处 1 可薄 龙压编四列大 9c 第代力大 ss 系 0 度薄 c 总锐力总大 可本代可 82 编 p 语至志薄 大珑压 m 最大 提 d9 戴 9 大 器器处战理大 p 言算 4 升薄 升总升系玲 度 3 达器玲 玲编 9 戴 9 大 列频码珑戴大 月度 m 尔可薄 言力高 d 理大 dm 视列 m 大 行性度频系薄 9p 力 p 编大 8 珑 2 码 c 大 语能最高编 高理可战可薄 6c1 珑 d 大 提 m 视列 m 大 四码 d 至志薄 升器 c 最 s 大 珑模件四频 2 3 大战缩系薄 能 8 力模语大 2 尔行模第 2 9 系轻文戴薄 月 1 缩行缩 2 速战编升 0 大",

"answer":"玲 c 可珑系薄 型 4 四视度大 最 8 薄语高 2 升 s 语 0 本薄 四缩器升件大 3a 第珑可大",

"_id":"6682d5c3cc160000370065f8"}]:

6.2 密文查询

查询“往来“,查询条件加密为

{"core":"yinhang",

"query":"达缩 1 锐可薄 件大视",

"skip":0,"limit":10,"byid":0,"flag":0}:

系统密文查询界面见图 3.

图 3 查询界面

服务器返回查询结果:

{"result":[{ "query":"达缩 1 锐可薄 件大视",

"w":"达缩 1 锐可薄 件大视",

"QTime":"0.003","numFound":1,"result":[{

"title_s" : "达缩 1 锐可薄 件大视",

"content" :"达珑玲行志薄 0 行戴码 1 大 运运 6i 战大 提 8 处 1 可薄 龙压编四列大 9c 第代力大 ss 系 0 度薄 c 总锐力总大 可本代可 82 编 p 语至志薄 大珑压 m 最大 提 d9 戴 9 大 器器处战理大 p 言算 4 升薄 升总升系玲 度 3 达器玲 玲编 9 戴 9 大 列频码珑戴大 月度 m 尔可薄 言力高 d 理大 dm 视列 m 大 行性度频系薄 9p 力 p 编大 8 珑 2 码 c 大 语能最高编 高理可战可薄 6c1 珑 d 大 提 m 视列 m 大 四码 d 至志薄升器 c 最 s 大 珑模件四频 2 3 大战缩系薄 能 8 力模语大 2 尔行模第 2 9 系轻文戴薄 月 1 缩行缩 2 速战编升 0 大",

"answer" :"玲 c 可珑系薄 型 4 四视度大 最 8 薄语高 2 升 s 语 0 本薄 四缩器升件大 3a 第珑可大",

"_id" :"6682d5c3cc160000370065f8" }]},"core":"yinhang","tm":"0.003"}

输入本地密钥解密见图 4 所示.

图 4　解密后结果

综上所述,本文利用可搜索加密技术,构建密文搜索系统,该系统可以实现金融交易信息密文的快速和安全的检索,提供了安全存储、安全传输和安全运算,并且计算的结果也是加密安全的,从而保证用户交易行为的数据、隐私、计算和分析的安全.

7　结论

1)结合码表和数学的进制转换,提出了码位分离的编解码方法,实现信息的加密和解密运算,采用码表的全排列形式作为密钥,为金融交易行为密文检索提供了可靠的同态运算方法.

2)基于路径散列的消息摘要方法,经过分组、分组散列、调和散列到摘要的字符串表示,实现了不可逆的消息摘要的生成方法.

3)提出了基于语句索引算法的全文检索系统,采用文字链式 hash 编码技术,实现了多语种的全文检索,为金融交易信息密文高效搜索提供了新途径.

4)结合同态算法的原理,构建密文全文检索系统, 实现了金融交易信息传输、存储和检索整个环节的信息安全.

参考文献:

[1] PRAWIRA F R, PRAKOSO N T, HANDAYANI P W, et al. The influence of information security factors on the continuance use of electronic wallet[J]. Procedia Computer Science, 2024, 234: 1467-1475.

[2] CHUN S H, CHO W, SUBRAMANYAM R. Transaction security investments in online marketplaces: an analytical examination of financial liabilities[J]. Decision Support Systems, 2016, 92: 91-102.

[3] 佚名. 数字经济与经济高质量发展:数字经济开放研究平台第二次学术研讨会会议综述[J]. 金融评论, 2023, 15(2):

118-123.

[4] 徐阳洋, 陆岷峰. 关于商业银行数字化转型模式实践与创新路径的研究:基于近年来部分 A 股上市银行年报分析[J]. 西南金融, 2022(8): 72-83.

[5] 黄杨杨. 属性 Logistic 混沌映射下的物联网隐私数据安全共享[J]. 现代电子技术, 2024, 47(13): 97-101.

[6] 张净, 唐恒睿, 刘晓梅. 基于区块链及 IPFS 的农产品多链追溯系统研究[J]. 中国农机化学报, 2024, 45(7): 127-134.

[7] DESHPANDE V, MUNDRU N, RATH S, et al. Data-driven surgical tray optimization to improve operating room efficiency [J]. Operations Research, 2023: 3866226.

[8] YEUNG J, VIRELLA PÉREZ Y I, SAMARASINGHE S C, et al. Study protocol: a pragmatic trial reviewing the effectiveness of the Transition Mate mobile application in supporting self-management and transition to adult healthcare services for young people with chronic illnesses[J]. BMC Health Services Research, 2022, 22(1): 1443.

[9] WANG M M, RUI L L, XU S Y, et al. A multi-keyword searchable encryption sensitive data trusted sharing scheme in multi-user scenario[J]. Computer Networks, 2023, 237: 110045.

[10] QIU J. Ciphertext database audit technology under searchable encryption algorithm and blockchain technology[J]. Journal of Global Information Management, 2022, 30(11): 1-17.

[11] 兰亚杰, 马自强, 陈嘉莉, 等. 基于区块链的可搜索属性加密技术应用综述[J]. 计算机科学, 2024, 51(S1): 870-883.

[12] 孙国梓, 王钰, 李兆维, 等. 基于区块链的可搜索加密技术研究综述[J]. 南京邮电大学学报(自然科学版), 2024, 44(1): 65-78.

[13] SHANTHI P, UMAMAKESWARI A. Privacy preserving time efficient access control aware keyword search over encrypted data on cloud storage[J]. Wireless Personal Communications, 2019, 109(4): 2133-2145.

[14] 迟佳琳, 冯登国, 张敏, 等. 隐私保护密文检索技术研究进展[J]. 电子与信息学报, 2024, 46(5): 1546-1569.

[15] 翁思扬, 俞融, 王清帅, 等. HTAP 评测基准的评测能力综述[J].软件学报, 2024,14(5):1-23.

[16] 肖泉彬, 陈源, 吴毅坚, 等. 基于代码克隆差异分析的函数模板挖掘和检索方法[J].软件学报, 2024,15(9): 1-21.