doi: 10.7690/bgzdh.2024.07.007

基于密文策略的电子档案快速加密方法

周　颖
（保定市人力资源和社会保障局人事考务中心，河北 保定 071000）

摘要：针对电子档案在保存过程中存在的安全隐患，提出基于密文策略的电子档案快速加密方法。从新增和更新 2 方面分析档案储存流程，利用量子通信技术建立安全信道，为档案和密钥传输营造安全的信道环境；使用密文策略构建快速加密模型，设置线性流程起点数量、安全参数等基本信息；将公共参数、流程访问结构作为输入，确定映射函数，生成密文；选取密钥生成算法的输入信息和组成要素，获得加密私钥；以密文和私钥为输入，推算出起点秘密，经递归操作运算出最终明文，完成快速加密。实验结果表明：该方法加密速度快，生成的密文较短，加密后的文档置乱性较强。

关键词：唯密文攻击；快速加密模型；密文策略；映射函数
中图分类号：TP391　　**文献标志码：**A

Fast Encryption Method of Electronic Archives Based on Ciphertext Strategy

Zhou Ying
(*Personnel Examination Center of Baoding Human Resources and Social Security Bureau*, *Baoding* 071000, *China*)

Abstract: In view of the security risks of electronic archives in the process of preservation, a fast encryption method of electronic archives based on ciphertext strategy is proposed. The archive storage process is analyzed from two aspects of new addition and update, and a secure channel is established by using quantum communication technology to create a secure channel environment for archive and key transmission; a fast encryption model is constructed by using a ciphertext strategy, and basic information such as the number of starting points of a linear process and security parameters is set; a public parameter and a process access structure are taken as inputs, and a mapping function is determined to generate a ciphertext; The input information and composition elements of the key generation algorithm are selected to obtain the encryption private key; the ciphertext and the private key are taken as the input, the starting point secret is calculated, the final plaintext is calculated through the recursive operation, and the fast encryption is completed. The experimental results show that the encryption speed of this method is fast, the generated ciphertext is short, and the encrypted document has strong scrambling property.

Keywords: ciphertext-only attack; fast encryption model; ciphertext strategy; mapping function

0　引言

档案是处理各类业务时生成的文件，是一种需要长久保存的记录。档案通常以实体方式存在，分为信件、账目和图像等形式。随着办公自动化要求的提高，企事业单位逐渐将文档通过电子文件形式呈现，与传统纸质档案相比，电子档案能够脱离载体，加强流通性，有利于提高数据的完整程度。但网络的连通性也给电子档案的安全带来新的考验，在复杂的网络环境下，难以保证通信绝对安全，档案在储存和传输过程中都容易被他人篡改或截取；因此，电子档案加密工作始终是该领域学者关注的重点。

文献[1]提出基于 CA 电子证书的电子档案加密防护研究。使用元数据与标签的档案管理模式，改善档案查询与分类效率，增强档案定位功能，设置私钥加密过程，利用 CA 电子证书提高网络环境的安全性，提高档案安全等级。文献[2]设计一种加密全息数字水印电子档案储存系统，确定系统整体架构，将硬件模块分为数据管理、用户管理、档案分类储存等模块，提高管理效率，利用加密全息水印技术对电子档案做去噪和水印提取，完成软件部分设置。

上述加密方法增强了电子档案管理的安全性，但由于档案规模呈爆炸式增长，降低了算法运行效率，增加了计算开销，同时大大减少了系统储存空间[3]。笔者基于密文策略，提出一种电子档案加密方法。密文策略是属性加密的一种，在加密明文时，将安全参数、公共参数、主密钥等作为不同步骤的输入[4]，获取加密后的密文，经过解密处理，得到

收稿日期：2024-03-25；**修回日期：**2024-04-21
第一作者：周　颖(1984—)，女，河北人。

明文信息。此外，笔者还利用量子通信技术为电子档案的储存与传输营造一个更加安全的环境，进一步提高档案的保密性。

1　基于密文策略的电子档案快速加密

1.1　电子档案的储存流程分析

分析电子档案的储存流程，能够得知档案在哪个环节更易遭到攻击，结合该环节特点，设置有针对性的加密算法。

对于档案管理系统而言，通常只有工作人员才具备录入与修改的权限，他们能够新增或更新电子档案内容。管理员将档案相关属性传输到逻辑层，利用访问层将档案保存在数据库等信息保护系统中。

档案储存的具体流程如如图 1 所示。

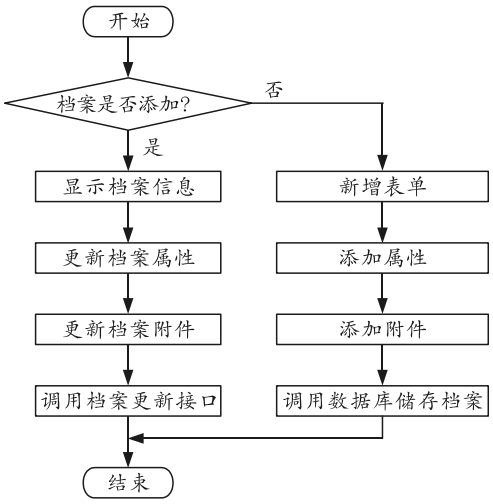

图 1　电子档案储存流程

步骤 1：判定待添加的档案是否已经存在数据库中，如果存在，在表单中显示该档案现阶段信息；若不存在，显示空白表单[5]，管理员录入此档案；

步骤 2：如果需要新增档案，管理员在新增列表中填写档案属性与附件信息[6]，提交表单，转到步骤 4 继续处理；

步骤 3：如果需要更新档案，管理员在更新列表中查找档案数据，更新属性与附件，提交表单，继续执行步骤 5；

步骤 4：逻辑层接收新增表单信息后，将附件和属性分别保存在磁盘和数据库中[7]，同时将这些信息利用 RESTful 接口传输到档案保护系统[8]；

步骤 5：逻辑层中档案更新模块接收更新申请后，将附件保存在磁盘内，替换原有附件，并更新档案属性，将更新后的信息利用 RESTful 接口发送到保护系统。

上述即为完整的档案保存流程，在这些步骤中，无论对于档案新增还是更新而言，当逻辑层接收操作申请后，在最后保存到磁盘与数据库的过程中，最易受到攻击。因此，要想实现快速加密，必须针对档案系统中逻辑层的相关特征，设计有效的加密算法。

1.2　攻击类型分析

电子档案会受到多种类型的攻击，攻击会导致电子档案的密码体出现缺陷。为全面防止攻击，需分析攻击类型和遭到攻击的后果。常见的密码攻击方式如表 1 所示。

表 1　密码攻击方式

攻击模式	攻击条件
唯密文攻击	只能获取部分加密密文
已知明文攻击	已知任意明文信息 明确和明文信息相互对应的密文
选择明文攻击	攻击者可以有针对性的攻击，例如选择对破译有帮助的明文
选择密文攻击	攻击者还可以选择特征明显的明文，例如图像等 选择对破译有帮助的密文 选取密文对应的明文

1.3　建立密钥传输安全信道

密钥是加密算法的关键[9]，要想保证密钥在安全环境下传输，必须营造安全的信道传输环境[10]。笔者利用量子通信技术构建密钥传输信道，确保加密算法在安全环境下实现。

量子信道的主要特征：保密性好，引入不可克隆性原理，在传输过程中如果被窃听，必定会发现；传输速度快，不会受物理障碍制约[11]，基本没有延时现象出现，时效性强。

量子通信在保障信息安全方面拥有突出优势，不但属于一类新的加密技术，还是解决信息传输安全的关键方法。现阶段，各国对量子通信非常重视，表明新的通信时代正在开启。

和经典通信方式相同，量子通信模型也分为信源、信宿、变换器等模块[12]。其中，信源是信息传输的载体，变换器将待传输的数据变换为量子比特，通过反变换器将量子比特还原成原始数据，获取最终的信源信息。在整个传输过程中，攻击者难以对量子信道进行攻击和破坏，且传输质量不受传输距离的制约。

利用经典信道配合量子信道，建立如图 2 所示的密钥传输信道模型。

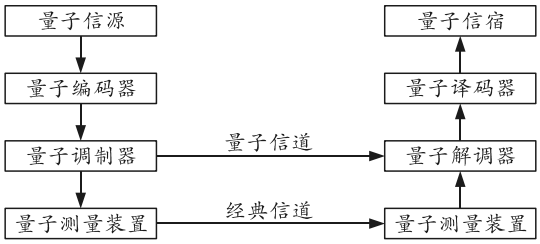

图 2　密钥传输信道基本模型建立

上图中，信源可将传输的信息变换为量子比特，起到生成器的作用；编码器主要工作是对量子比特做编码处理，减少噪声干扰；调制器负责调制比特流，确保比特流更加符合信道特征，提高传输质量；解调器主要对量子信息解调，获取调制前的量子；译码器属于信息解码工具[13]。量子与经典信道的作用分别是传输量子信号和传输其他信息。

此种通信方式在经典信道的配合下，可更准确地判断出密钥传输过程中是否被监听，增加通信可靠性，保证密钥安全。

1.4　基于密文策略的快速加密模型构建

在上述建立的安全信道下，利用密文策略构建快速加密模型，该模型共包括基础设置、加密、密钥生成和解密 4 个子算法[14]，具体建模过程如下。

1) 设置。

在设置过程中，将安全参数 N 作为算法输入，设定线性流程起点数量 B 和关系集合 R。任意选择某素数 $p>2^N$，建立与 p 阶相关的 2 个群 G 和 G'，令 $e:G\times G\to G'$ 是双线性映射，且群 G 中的某生成元表示为 g，选取 B 个群 G 中的元素 $h_j\in G\left(j\in\{1,2,\cdots,B\}\right)$，将其当作流程起点。针对关系集合 R 内某关系 $(t\to k)\in R$，对应的选出 G 中元素 $r_{t,k}\in G$，以其为公共参数。挑选随机参数 $a,b\in Z_p$，Z_p 是随机素数集合，计算 $a,b\in e(g,g)^a,g^b$。

2) 加密。

在加密算法中，公共参数 P、档案访问结构 A 以及消息 M 作为输入。其中，A 包含某个具有 i 行 n 列的矩阵 $\boldsymbol{U}$，流程起点和终点集合分别表示为 $\Im$ 和 D，在关系集合中挑选出映射函数[15] ρ，ρ 能够将 $\boldsymbol{U}$ 中所有行映射在流程终点集合元素中。

选取随机数 $s\in Z_p$，生成如下密文：

$$\left.\begin{aligned}C_M&=M\cdot e(g,g)^{as}\\C_0&=g^s\end{aligned}\right\}。\tag{1}$$

式中 C_M 和 C_0 均为密文组成元素。

3) 密钥生成。

将主密钥 MSK=(a, b)、线性流程起点集合 $\Im$ 和关系集合 R 作为输入。

选取任意随机数 $t\in Z_p$，计算：

$$\left.\begin{aligned}K&=g^ag^b\\K_0&=g^s\end{aligned}\right\}。\tag{2}$$

针对起点集合 $\Im$ 和关系集合 R，计算：

$$\left.\begin{aligned}K_j&=h_j:(\forall j\in\Im)\\r_{t,k}&:\left(\forall(t\to k)\in R\right)\end{aligned}\right\}。\tag{3}$$

式中 K、K_0 和 K_j 均为密钥组成要素，则最终的密钥输出为：

$$\left.\begin{aligned}\mathrm{SK}&=(K,K_0)\\K_j&=(\forall j\in\Im)\\K_0&=\left(\forall(t\to k)\in R\right)\end{aligned}\right\}。\tag{4}$$

式中 SK 表示私钥。

4) 解密。

解密过程中，将密文 CT 和私钥 SK 作为输入。

如果 L 表示私钥 SK 中符合密文 CT 定义的线性流程集合，为方便描述密钥生成和解密算法之间的关系，假设 L 包含 2 个线性流程分别是 $L_0\to L_1\to L_2$ 与 $L_3\to L_4$。在密钥生成过程中，已知起点 L_0 和 L_3 以及关系 $L_0\to L_1$、$L_1\to L_2$ 和 $L_3\to L_4$ 的密钥，而在解密算法中也会已知这些条件。此外，还会得到终点 L_2 和 L_4 的密文；因此，密钥生成与解密过程缺一不可，如果密钥生成算法没有产生密钥，则说明没有完成流程 $L_0\to L_1\to L_2$ 和 $L_3\to L_4$；若解密算法没有公布密文，表明无法解密。终点 L_2 和 L_4 中包括主秘密 f 的合法分割，因此集合 L 是私钥 SK 中符合访问结构的线性集合。

如果私钥 SK 中的流程集合符合访问结构相关要求，解密成功，具体解密过程如下。

如果子秘密 λ_i 表示对秘密 s 的分享，选择一个秘密向量 y 确保下式成立：

$$\sum_{i=1}y\lambda_i=s。\tag{5}$$

假设集合 L 内随机挑选一个流程表示为 $\mu_0\to\mu_1\to\cdots\to\mu_{l-1}\to\mu_l$，通过下式推算出起点 μ_0 的秘密 T_k：

$$\begin{aligned}T_k&=(\mu_{0,1},K_0)\cdot(\mu_{0,2},K_{\mu_0})^{-1}=\\&(D_{\mu_0},g^a)\cdot(g^b,\mu_0)^{-1}=(g,D_{\mu_0})^{-1}:(\mu_0\in\Im)。\end{aligned}\tag{6}$$

结合上述获取的 μ_0 秘密值 T_k 后，继续执行递归运算，推导出 T_{k+1}：

$$T_{k+1}=T_k\bullet(C_m,C_0)\bullet(\mu_k,K_{\mu_k})=(g,D_{\mu_k})^{-1}\bullet(D_{\mu_k}^{-1}D_{\mu_{k+1}})=(g,D_{\mu_{k+1}})。\tag{7}$$

因 λ_i 属于秘密 s 的分享，结合式(5)可得：

$$\prod_{i\in f}s\left(g^a,g^b\right)^{\lambda_i}=\sum_{i\in f}\lambda_i 。\tag{8}$$

利用下述公式即可计算出明文：

$$m=\frac{C_M}{(K_0,C_0)}/\prod_{i\in f}(g^a,g^b)^{\lambda_i} 。\tag{9}$$

计算出明文后即可获得电子档案的真实信息，建立一个完整的快速加密模型。

2 实验数据分析与研究

为证明所提方法对电子档案加密的有效性，利用分层方式搭建实验平台，该平台由界面层、逻辑层与访问层 3 个模块构成。其中，界面层可以为实验人员提供操作界面，逻辑层属于中间层，将用户请求变换为具体业务，再利用访问层实现相应操作。实验平台整体架构如图 3 所示。

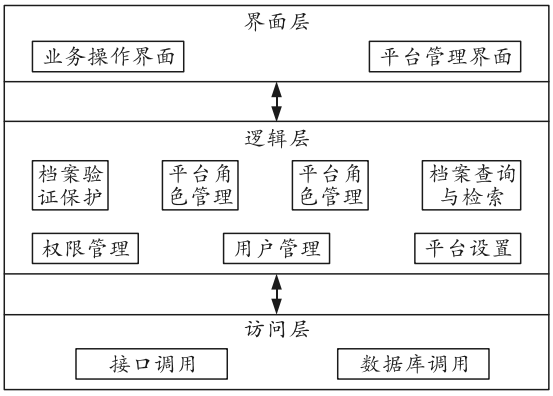

图 3 实验平台整体架构

以某企业单位为例，定义该企业电子档案系统模型，包含如下部分：

1) 服务器：为半可信状态，负责档案储存和处理用户请求，它能够执行委派的任务，但也对加密内容感兴趣。它和攻击者的本质区别是不会进行主动攻击。

2) 授权中心：为完全可信状态，主要作用是分发密钥，所有参与方都能信任它。

3) 档案持有者：是唯一可以对档案授权的用户，具备读取操作密钥，但没有更改权限。

4) 档案修改者：拥有档案的写操作权限，如果持有者对其授权，也可以具备读操作权限。

5) 档案阅读者：属于最普通的用户，经过持有者授权后，仅有查询的权利。

该企业档案管理系统模型如图 4 所示。

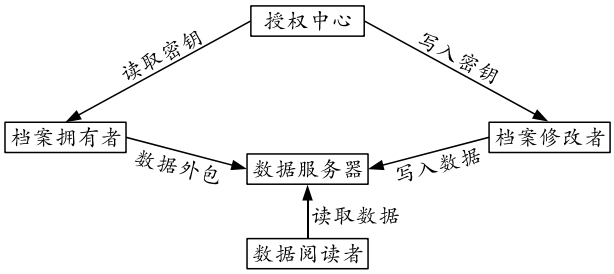

图 4 企业电子档案系统模型

为更好地完成此次实验，设定如下安全假设：

假设 1：第三方为完全可信的；

假设 2：服务商是不完全可信的，虽然不会随便泄露档案信息，但是可能会窥探档案内容；

假设 3：具备查询权限的用户不会将个人数据与档案信息泄露给其他用户。

在上述条件下，首先建立档案序列，如图 5 所示，利用基于密文策略的加密方法对档案加密，加密后的档案输出情况如图 6 所示。

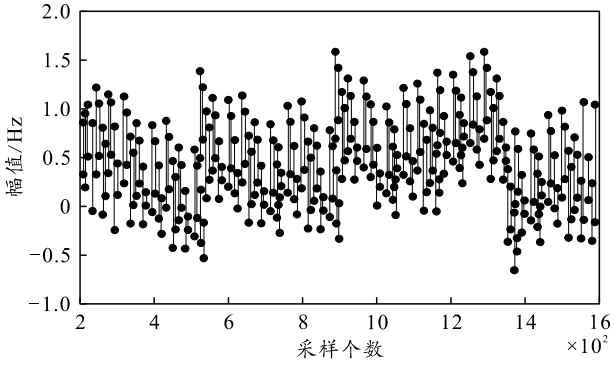

图 5 加密前档案序列

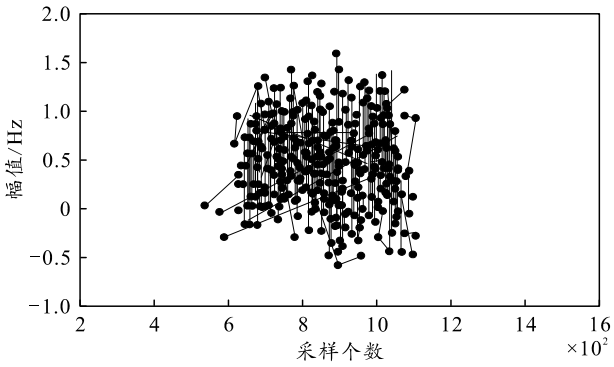

图 6 加密档案输出结果

分析上图能够得出，经过密文策略加密后的输出文档具有较强的置乱性。加密前，文档序列较为规整，抗攻击度较差，攻击者可轻易获得明文信息；而加密后的文档看不出序列形式，提高了文档的保密性，不易读取或篡改。

要想实现文档快速加密，必须分析算法的计算开销，主要表现在加密时间和密文长度 2 方面。为

凸显本文中方法的优势，分别分析本文中方法、CA 电子证书加密、全息数字水印加密算法的计算开销，测试结果如图 7 和 8 所示。

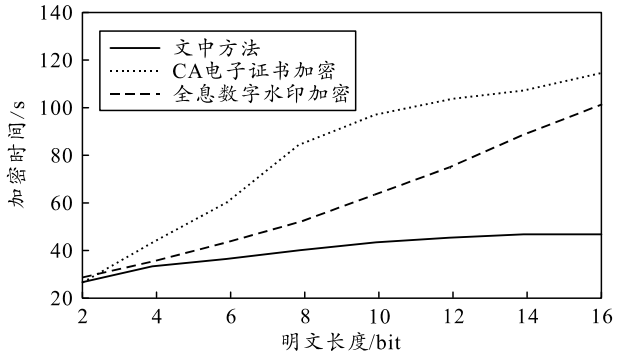

图 7　不同方法加密时间对比

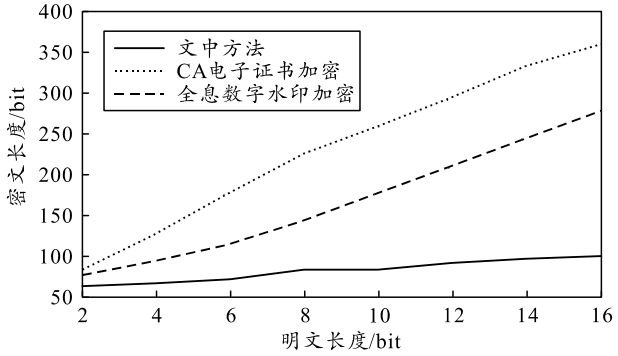

图 8　不同方法密文长度对比

分析上图可知，随着明文长度的增加，文中方法的加密时间和密文长度没有出现明显的上升趋势，而其他 2 种方法的加密时间和密文长度曲线上升幅度较大，说明算法计算开销花费较多。另外密文长度还能表现出加密算法所占内存情况，本文中方法的密文长度始终较少，证明该方法在加密过程中不会对系统造成较大负担，减少了系统内存。这是因为基于密文策略的加密方法无论是密钥生成过程还是解密过程都非常简单。

3　结论

笔者利用密文策略研究一种电子档案快速加密方法。建立量子通信系统模型，为密钥和密文传输提供安全的通信环境，结合密文策略，实现电子档案的加密。实验结果表明，该方法能够减少计算开销，提高文档的抗攻击性，为电子档案加密研究提供参考。

参考文献：

[1] 李莉. 大数据环境下个人数字档案的分类管理与加密防护研究[J]. 档案管理, 2021(6): 57-58.

[2] 王晓琴. 基于加密全息数字水印技术的电子档案管存系统设计[J]. 现代电子技术, 2021, 44(8): 81-84.

[3] 刘洪, 罗茜. 关于新技术热潮下在档案领域应用区块链技术的冷思考[J]. 北京档案, 2020(9): 15-18.

[4] 马仁杰, 沙洲, 罗吉鹏. 论区块链思维下我国档案信息服务模式的优化路径[J]. 档案学研究, 2021(4): 94-99.

[5] 袁芳, 张志刚. 多媒体平台视角下档案信息管理体系构建研究—以房产档案为例[J]. 情报科学, 2020, 38(11): 51-55.

[6] 钱秀芳, 赵小荣. 区块链技术在高校档案工作中的应用研究[J]. 档案与建设, 2021(11): 59-62.

[7] 张玉磊, 文龙, 王浩浩, 等. 多用户环境下无证书认证可搜索加密方案[J]. 电子与信息学报, 2020, 42(5): 1094-1101.

[8] 韩培义, 刘川意, 王佳慧, 等. 面向云存储的数据加密系统与技术研究[J]. 通信学报, 2020, 41(8): 55-65.

[9] 陈宏君, 蒋建军. 基于光通信技术的物联网数据加密技术研究[J]. 激光杂志, 2021, 42(5): 116-119.

[10] 李俊, 蒋德勇, 王文娟, 等. 基于空间稀疏编码的电子通信数据链加密仿真[J]. 计算机仿真, 2021, 38(8): 190-193, 221.

[11] 陈家豪, 殷新春. 基于云雾计算的可追踪可撤销密文策略属性基加密方案[J]. 计算机应用, 2021, 41(6): 1611-1620.

[12] 马潇潇, 黄艳. 大属性可公开追踪的密文策略属性基加密方案[J]. 计算机科学, 2020, 47(S1): 420-423.

[13] 荀艳梅, 陈燕俐, 彭春春. 支持多跳的多策略属性基全同态短密文加密方案[J]. 南京邮电大学学报(自然科学版), 2021, 41(6): 101-112.

[14] 赖霖汉, 缪祥华. 基于雾计算的权重 OBDD 访问结构属性密码体制研究[J]. 电视技术, 2021, 45(8): 95-101.

[15] 黎琳, 张芳, 张闻宇. 一种实现数据库同态计算的 ELGamal 重加密算法[J]. 北京交通大学学报, 2021, 45(2): 127-134.