基于量子安全服务平台的数据库加密技术

陈云帆，蔡敏
（中国电信股份有限公司上海政企客户支撑响应中心/量子能力中心，上海 200041）

摘　要：如今，企业的数据安全问题屡见不鲜，数据泄露事故频发。数据库安全目前已经成为企业数据安全的重点关注内容，企业对于更高安全性的数据库加密需求越发迫切。量子密码服务平台是量子安全能力基础设施，可以为用户应用提供国密算法与量子密钥分发服务，本文主要对基于量子密码服务平台的数据库加密的技术展开研究，并介绍企业利用量子技术为数据库加密的建设思路。

关键词：数据库加密；策略管理平台；量子安全服务平台（CSP）；AOE插件
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000-0801.2025074

0　引言

现代信息系统在数据存储设计的时候需要考虑许多安全因素，包括数据库受攻击面大小，数据库访问涉及的认证、授权和审计问题，从网络层面做了很多的安全措施，但由于开发人员疏忽带来的软件漏洞和运维人员的管理不善等因素，使得漏洞总是不可避免，各种各样的风险都可能出现并带来可怕的后果，如图1所示。

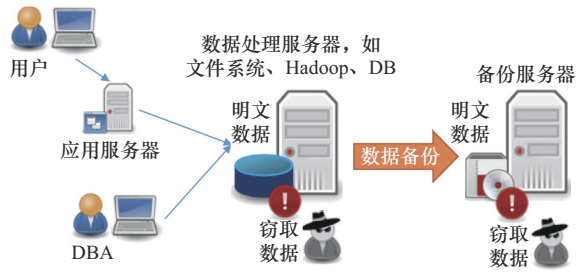

图1　存储的数据面临被窃取的威胁

攻击者通过攻击数据库服务器，窃取集中存储的个人敏感信息数据，在数据本身没有做加密等安全防护措施的情况下，风险极大。

针对数据存储的威胁不难看到，只有对数据本身进行加密，让数据以密文的形式存在数据库中，才是最直接有效的防护手段。采用基于国密算法的加密技术，可防范数据被窃取的风险，做到防“拖库”，防越权，如图2所示。

1　数据库加密核心诉求与难点分析

（1）对敏感数据进行加密保护

为加强对数据资产的保护，防范数据被窃取的威胁，维护组织机构的声誉和利益，需要使用密码技术对数据进行安全保护。

（2）应用免开发改造

通过应用开发改造的方式来实现数据安全防护，需要投入大量的工作，而且已经上线运行的系统经过安全底层的改造，势必带来较大的风险，会影响正常业务的开展。因此，需要一种应用系统免改造的方案，较短周期、较低风险地实现数据安全防护效果。

（3）密码技术具备高性能

大数据量的高速流转，以及业务的持续不间

收稿日期：2024-11-10；修回日期：2025-03-02

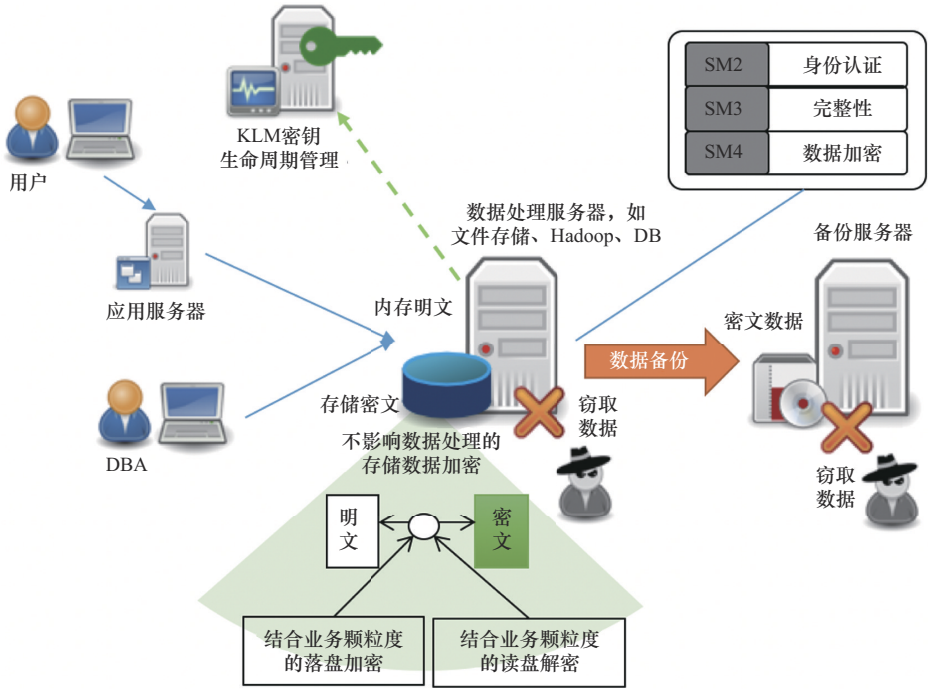

图2　使用密码技术保护存储的数据

断、高可用，要求应用的密码技术具备高性能以及高可用性。

（4）兼容各种数据库品牌和版本

在改造中，不可能针对每个数据库都要实现一种专门的方案，需要一种方案无关数据库品牌和版本，并以统一方式实现数据库中数据安全。

（5）统一管理可扩展

数据来源于信息系统的采集和产生，并在各个信息系统和业务单位间流转，建设的密码防护体系能够统一管理各个信息系统的安全功能，并且随着信息化的发展，对于新建设的系统也能够纳入管理的范围内。

（6）建设数据安全防护体系

通过顶层规划，面向业务的全局，构建数据安全防护体系，建设安全服务平台，持续为业务的运营保驾护航。

（7）满足合规要求

遵循密评以及等保等的合规要求，采用国密算法，保护重要数据的机密性、完整性等，实现对“应用与数据安全”中的各项需求满足。

2　数据库加密技术与建设思路

2.1　量子数据库加密技术结构总揽

建设量子数据库加密系统，与业务系统对接，针对具有重要价值的敏感数据，基于商用密码算法高性能实现进行加密保护。量子密码服务平台功能架构如图3所示，该平台能以免应用改造的方式，实现对业务应用系统中结构化数据的存储加密，提供有效且易于实施的数据安全保护在网络架构上，量子密码服务平台提供数据库加密的密钥源，与策略管理平台对接。策略管理平台用于制定量子数据库加密策略，并对接AOE插件。量子数据库加密系统部署示意图如图4所示。

AOE数据加密插件（以下简称AOE插件）中包含高性能国密套件，即可实现以下安全保护目标。

- 实现免开发改造应用系统，实现增强业务应用的数据安全能力的同时，而不影响现有业务系统的稳定性，保证已上线系统的正常运营、不中断。

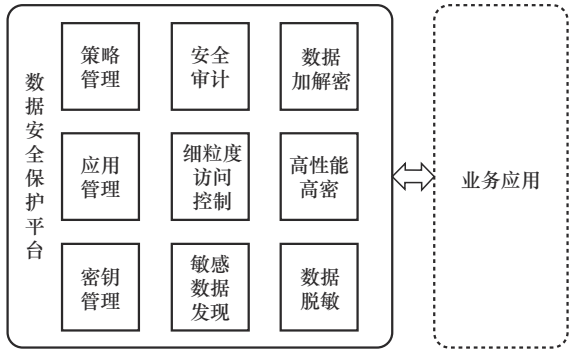

图3　量子密码服务平台功能架构

- 支持的应用系统环境包括本地物理机部署环境、虚拟机环境以及云环境。
- 实现进入数据库的结构化敏感数据的加密，防止数据库被拖库。
- 支持规模化部署，适应分布式大数据应用场景。

2.2　量子数据库加密系统建设内容

量子数据库加密系统示意图如图5所示。量子数据库加密系统由AOE插件、策略管理平台、量子安全服务平台组成。其中AOE插件部署在应用服务端，策略管理平台部署于业务系统同区域网络，量子安全服务平台已与策略管理平台网络可达。

2.2.1　AOE插件

数据安全插件原理示意图如图6所示。AOE插件部署在应用的服务端，只需要进行简单配置，应用无须再进行任何额外修改，即可向数据库存储密文，并且可对敏感重要的数据进行完整性保护。通过获取量子密码服务平台下发的策略规则，包括加密规则、访问控制规则、脱敏规则等。

数据安全防护模块包含高性能国密套件，可实现基于SM4算法的高性能数据加密。

AOE插件按照获取的安全策略，对从应用写入数据库中的数据进行加密，使数据以密文形式存储于数据库中，可防范数据库被拖库的威胁。

量子数据库加密系统采用了面向切面的密码技术，如图7所示，通过不修改原应用系统源代码的情况下，在应用系统的服务层与数据层之间

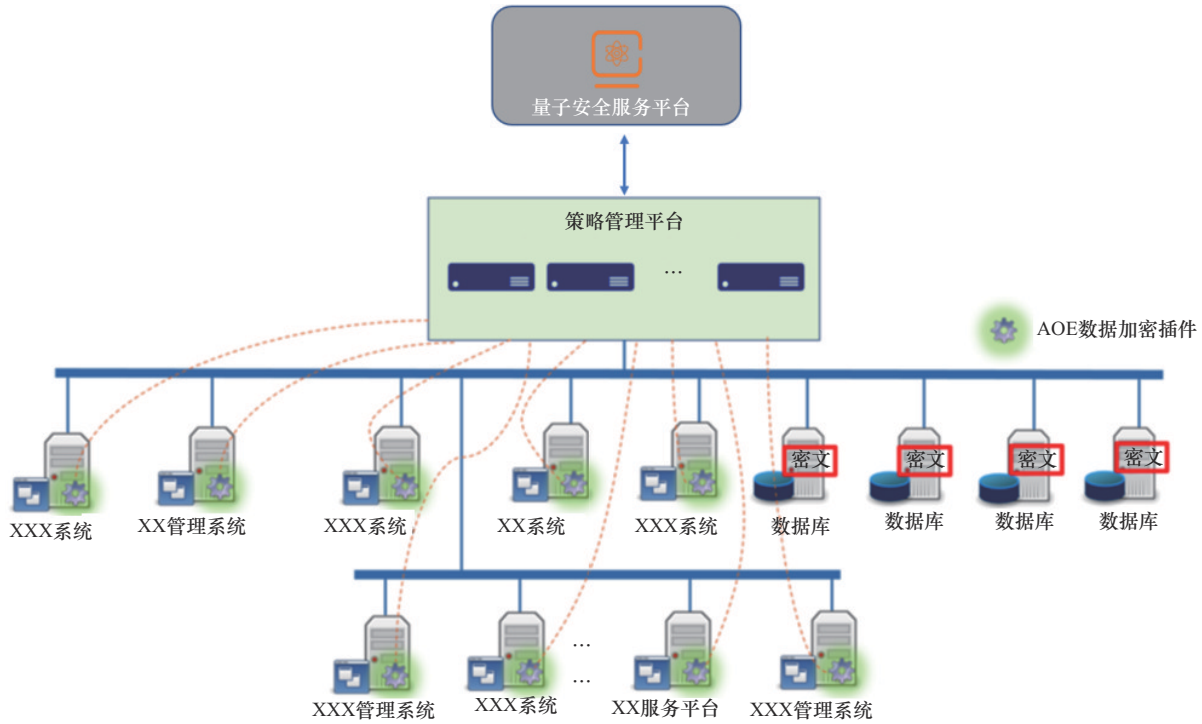

图4　量子数据库加密系统部署示意图

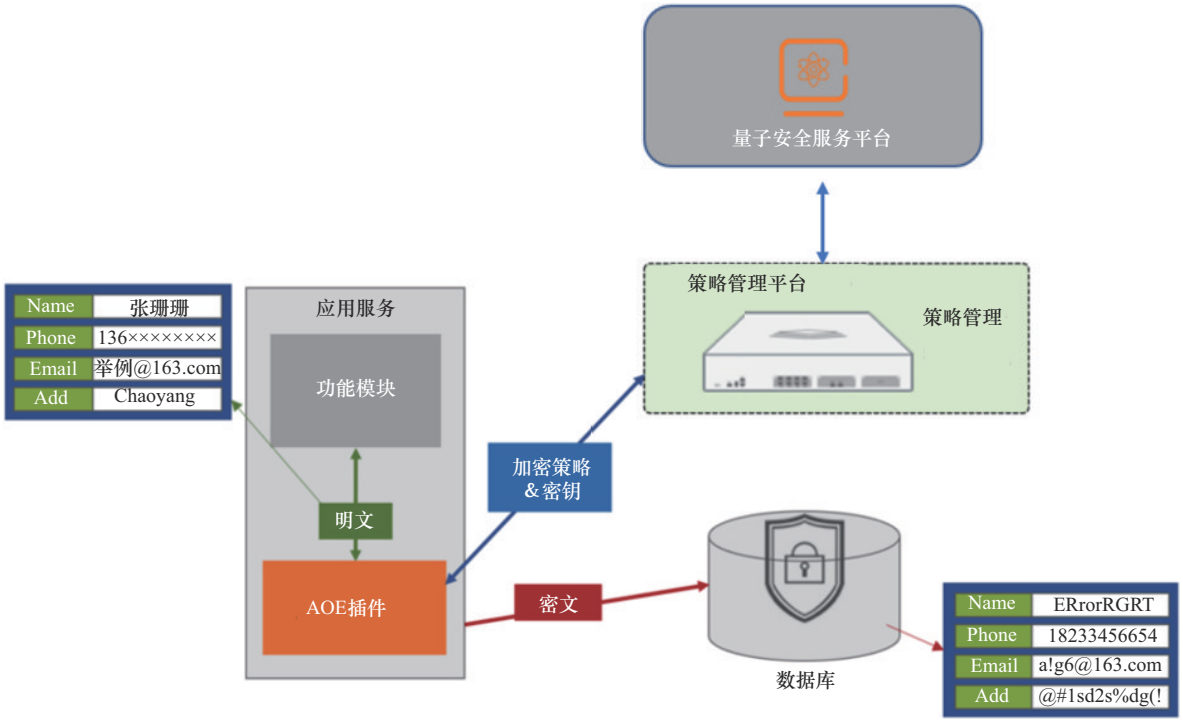

图5　量子数据库加密系统示意图

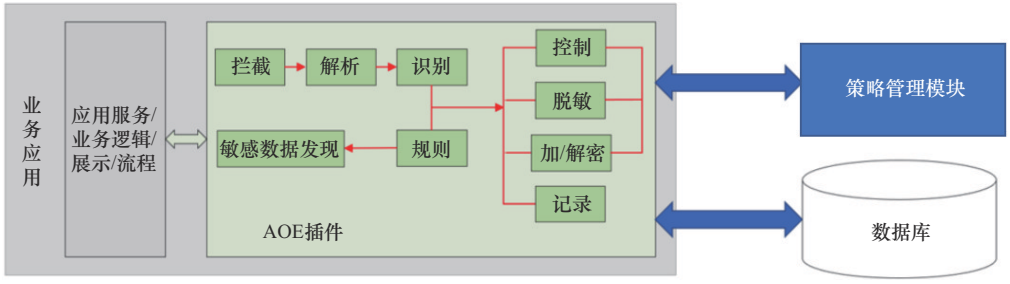

图6　数据安全插件原理示意图

“切入”了安全插件层，该层包装了原应用的数据库访问驱动，从而实现针对数据的安全防护的能力。

2.2.2　策略管理平台

策略管理平台基于B/S架构设计，通过浏览器登录管理界面进行系统和管理策略的设置。

数据安全策略管理平台功能示意图如图8所示，模块架构分为表示层、业务层和数据层，其中表示层提供核心的可视化管理控制台，以供管理员开展工作；业务层是事务处理的核心层，主要进行数据安全防护业务逻辑的处理；数据层是基础的持久层，为上层提供基础的数据存储服务。

策略管理平台旁路部署，管理员通过可视化管理控制台进行加/解密权限规则的设置，颗粒度可以达到数据库表的列级，加密策略的内容包括选择要加密的字段，以及所使用的加密算法，是否进行保留格式的加密。

2.2.3　量子安全服务平台

量子安全服务平台可提供量子安全服务能力，负责加/解密所需的密钥的管理工作，提供对密钥进行全生命周期管理的功能，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以及安全管

图7　面向切面的密码应用技术

图8　数据安全策略管理平台功能示意图

理等。量子安全服务平台组成如图9所示。

密码服务平台部署于服务器密码机集群和应用系统之间，托管应用系统的密钥，代理应用系统密码运算，管理服务器密码机集群；实现基于

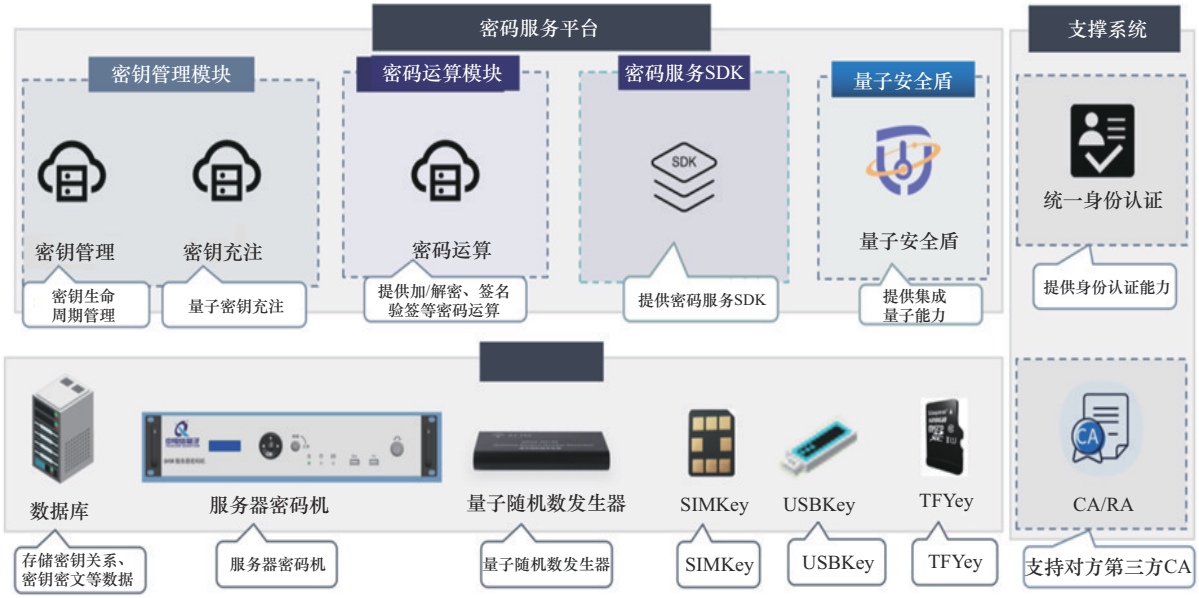

图9　量子安全服务平台组成

国密算法的密钥体系构建、密钥全生命周期管理的相关功能，根据业务需要提供密码运算接口；实现应用接入管理，支持多应用接入；实现服务器密码机设备管理与设备监控。

密码服务平台由密钥管理模块、密码运算模块以及密码服务SDK等组成。

（1）密钥管理模块

提供密钥生成、密钥分发、密钥充注、密钥更新、密钥销毁、密钥同步等密钥全生命周期管理，密钥类型包括接入平台的业务应用配置的对称密钥和非对称密钥、SIMKey的量子充注密钥和移动终端通话加密的会话密钥。提供用户、单位、应用授权等管理功能，提供设备注册认证等管理功能，提供服务监控、日志监控、密钥监控、设备监控、统计分析等功能。

（2）密码运算模块

提供数据加/解密、摘要生成校验、公钥加密/私钥解密、签名验签、会话密钥生成等密钥运算功能。

（3）密码服务SDK

提供密码服务SDK供接入应用对接，支持JAVA、C语言。

量子安全服务平台采用三级密钥派生机制，三级密钥即根密钥、模块密钥、工作密钥。根密钥和模块密钥均是由量子服务器密码机产生的真随机数。根密钥用于加密保护模块密钥。根密钥根据门限算法加密后导出至5个USBKey中，任意3个即可还原根密钥。模块密钥用于派生工作密钥，支持实现“一字段一密钥”，即数据库中每个字段使用不同的工作密钥进行加密，保证数据的机密性。工作密钥用于数据的加解密。模块密钥由根密钥加密后存储；工作密钥则由模块密钥实时派生，不落盘存储，从而保证密钥的安全性。

2.3　量子数据库加密建设研究案例

本次上海电信采用本地的塔台业务监控系统进行数据库加密。业务系统为上海电信政企塔台系统（测试环境版本），加密字段用户信息表为OA账号、姓名、手机号、电子邮箱字段。塔台系统网络架构如图10所示。数据库加密测试拓扑如图11所示。

本次建设内容如下。

（1）调用上海量子城域网内已建设量子密码服务平台（CSP）已建设能力，通过ENI网络获

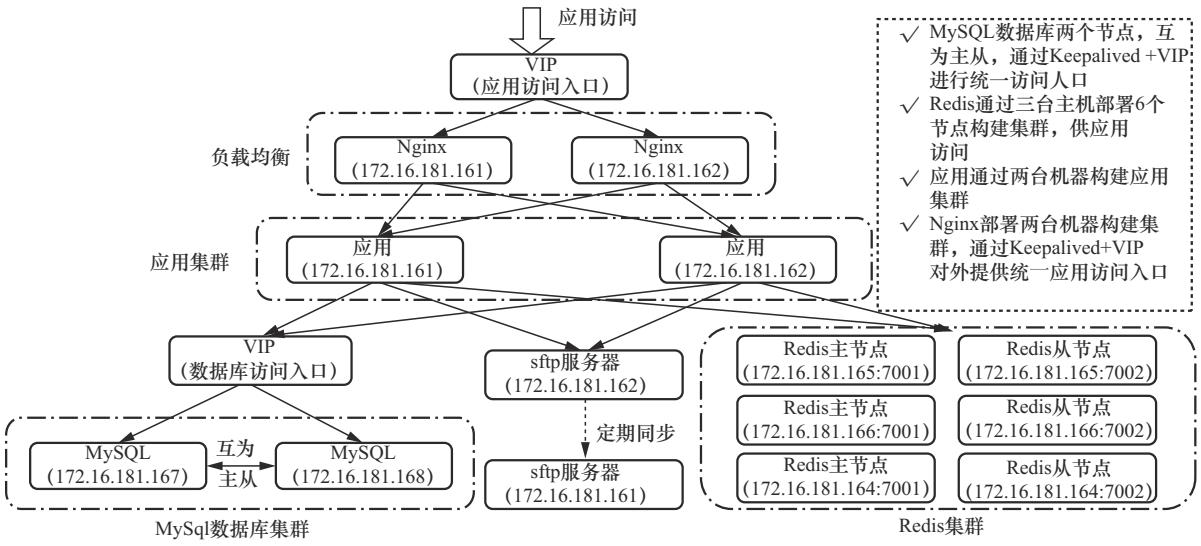

图 10　塔台系统网络架构

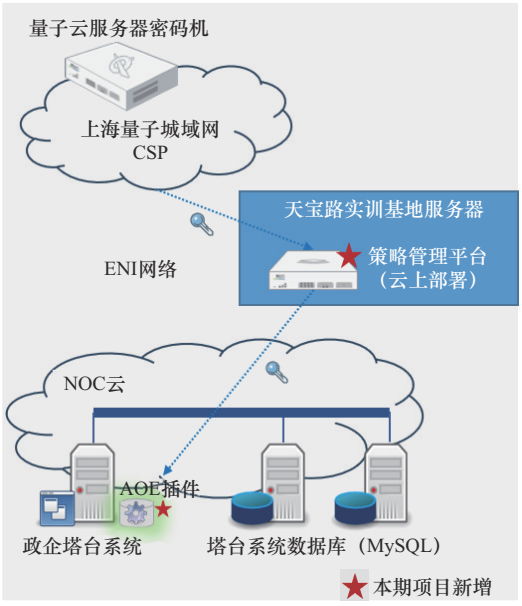

图 11　塔台数据库加密网络拓扑

取量子密钥。

（2）服务器上新增 1 套量子数据库加密策略管理平台，为插件执行统下发加解密及脱敏策略，负责统管理加/解密所需的密钥，实现密钥全生命周期的管理，保障密钥的安全备份与恢复。

（3）在政企塔台应用系统服务端的节点上分别部署 AOE 插件，满足结构化数据加密。

CSP 与策略管理平台的对接如下。

（1）在 CSP 平台创建数据库加密应用，为用户提供 AppID 与 AppKey。

（2）在策略管理平台的调度系统，/租户管理/租户详情/配置信息/密管配置中，为用户添加 app-id 与 app-key，选择密管类型为量子 CSP-Server，并配置 CSP 的服务地址，从 CSP 平台获取密钥。

（3）在策略管理平台的 CASB 系统中添加与策略平台数据库配置相同信息的数据源后，为应用添加相关的插件，下载 JAVA 插件到 tomcat 目录/data/app/apache-tomcat-9.0.86/webapps/gesc/WEB-INF/lib 中，并修改应用 JDBC 参数，即可完成与平台的对接。

AOE 插件的适配如下。

（1）解压缩 AOE 插件。

（2）安装 AOE 插件。

（3）加载环境变量，登录 CASB 安全平台，利用插件管理，新增应用，并绑定相关联的数据源。

（4）下载 AOE 插件并部署到应用。

（5）修改 aoelog.xml。

（6）配置 cg-casb.properties。

（7）修改应用 JDBC 参数。

提取表结构。登录 CASB 安全平台，下载 AOE-client 部署包，上传到 CASB 安全平台所在

主机或其他网络相连的LINUX主机上，安装部署AOE-client，然后利用extractor工具提取测试库表结构到CASB安全平台。

2.4 量子数据库加密建设成效

2.4.1 结构化数据存储加密

针对数据库中存储的结构化数据，量子数据库加密系统可以实现重要敏感字段的加密保护，具体实现功能如下。

（1）根据单位分类分级的结果或者实际需求，选择对重要敏感字段进行加密。即使数据库文件被非法复制或者存储文件丢失，也不会导致真实敏感数据的泄露。

（2）能对结构化数据实现精确到字段级的精细化防护，对于没有授权的用户绕过数据加密插件，即使窃取硬盘或复制数据也无法解密读取，可有效做到“防拔盘、防拖库”。

（3）支持国密SM4算法，可对不同字段采用不同加密算法不同密钥进行加密。

（4）对手机号、身份证号、Email等有固定格式的字段能实现保留格式的加密。

针对结构化数据存储加密是量子密码服务平台的核心功能。数据加密本质上是将一个明文数据经过加密密钥及密码算法转换，变成无意义的密文数据。通过加密技术保护数据安全，就是将数据的安全问题缩小到了密钥的安全，数据的安全就等同于密钥的安全。

数据加密后，只要具备以下3个条件，加密的数据就能够被解密还原。

- 加密后的密文保存完好，可通过单位既有的数据备份机制保证。
- 密钥保存完好，量子安全服务平台具备密钥安全管理机制。
- 使用了国家认可的密码算法（SM4），商用密码算法是量子密码服务平台的核心功能。

另外，数据加密后会在密文中添加密文标识，可保证明文不会被二次解密，密文不会被二次加密。在加密功能上线过程中，数据库中不可避免会出现明密文混合的情况，可通过明密文标识将明文和密文区分开。

2.4.2 数据库写入加密程序

数据库单条数据写入程序如图12所示。

图12 数据库单条数据写入程序

2.4.3 数据动态脱敏

平台可以在数据解密节点上，对敏感数据通过设置遮掩等方式实现动态脱敏，可实时将脱敏后的结果展示在应用前端。

动态脱敏是在生产环境中应用读取敏感数据的过程中实现，先经过插件解密，接着由插件根据脱敏策略进行脱敏，再将脱敏后的结果返回应用前端，性能上不影响正常业务，用户无延迟感知。

动态脱敏的基本原理是通过脱敏算法将敏感数据进行遮蔽、变形，将敏感级别降低后对外展示。插件中包含脱敏引擎，引擎中内置了常用的脱敏算法，并且支持根据用户需求定制脱敏算法。解密后的敏感数据由脱敏引擎根据已经设置的脱敏算法进行计算处理，得到脱敏后的结果返回应用前端展示。可以支持根据用户业务需求进行定制脱敏算法。

2.4.4 历史存量数据全量加密

量子密码服务平台可支持对应用系统已有的历史存量数据进行全量加密，可以一次性将相应数据库中已经存在的敏感数据进行批量加密，历史数据全量加密如图13所示。

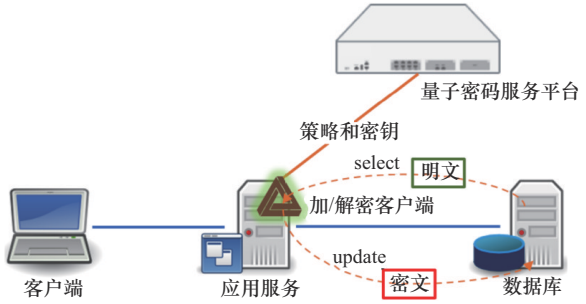

图 13　历史数据全量加密

批量加密是由加/解密客户端执行，加/解密客户端同加/解密插件一样，从管理平台进行下载（实施时由实施方下载，也可经过培训由甲方操作）。客户端与管理平台交互，获取要加密字段的策略和密钥，并执行全量加密，客户端先把敏感数据从数据库中读取（select）出来，经过加密处理形成密文后再更新（update）到数据库中，直到把目标数据库表中的敏感字段全部加密。全量解密的过程与全量加密相同，只是在客户端执行环节是解密计算，把读取的密文解密成明文后，更新到数据库中，直到目标数据库表中的密文字段全部解密完成。

2.4.5　密文模糊查询

密文模糊查询功能，是一种基于 GCM 加密模式的数据库加密字段模糊检索方法。通过将已加密字段的原始明文按照指定长度或长度序列进行分割，并应用基于 GCM 加密模式的加密算法，对明文分割后形成的各个片段进行加密操作，求取对应的认证值 Tag，生成对应的密文索引集合，将密文索引集合中的认证值 Tag 与密文拼接在一起，存储在密文字段中。在进行模糊检索时，利用密文索引集合中的元素与待检索内容进行匹配，既可以过滤掉大量不匹配记录，降低需要解密进行模糊匹配的记录数，提高查询效率，又由于应用 GCM 加密模式，可以灵活选择认证值 Tag 长度，从而对于数据库字段存储空间具有强适应性。另外，由于多因素参与，算法复杂性高，从索引逆向推导出原文基本无法实现，能够有效确保模糊检索时的数据安全。

密文模糊查询流程如图 14 所示。

2.4.6　基于国密算法的数据加密

本技术方案在功能实现中支持国密算法的应用，包括 SM2、SM3 以及 SM4，并且在加/解密性能与安全性上获得了突破，低延时高吞吐，可以轻松应对大数据量场景下的加/解密，消除用户在使用国密中的性能顾虑。

特别地，本方案支持基于 SM4 的保留格式的加密，即针对手机号码、身份证号等带有格式要求的字段内容，可在加密后仍然保留原字符的格式意义。目前该加密方式也已实现性能的优化，按业内水平，在单颗 CPU 环境下的性能可达到每秒钟格式保留加密 5 000 万条手机号码。

高性能国密套件参考了 OpenSSL 的框架，利用了 Engine（引擎）机制。

引擎机制是 OpenSSL 预留的用于加载第三方加密库的机制。一个软件或硬件的引擎库可以提供一系列计算方法的集合。用户可以实现一个 ENGINE 的数据结构，该结构包含一个引擎库的全部信息。

机制提供的 EVP 通用接口，能够通过引擎方式与加密库或加密设备协调工作，用软硬件提供的算法替换 OpenSSL 中原有的密码算法，从而使 OpenSSL 能够透明地使用第三方提供的软件库或者硬件加密设备进行加密。

2.4.7　密钥安全性说明

（1）内存中的保护机制

密钥在内存中工作时是处于明文状态，因此需要对密钥进行内存中的保护。安全插件在运行过程中，采用内存锁和内存清空机制，使密码模块独占一块内存，其他进程无法读取内存中的数据。使用结束后，对内存及时清零，从而保证了密钥的安全。内存锁将进程的部分或全部虚拟内存锁定到物理内存，被锁定的内存不会被调度到交换空间（swap space）。系统分配内存到页

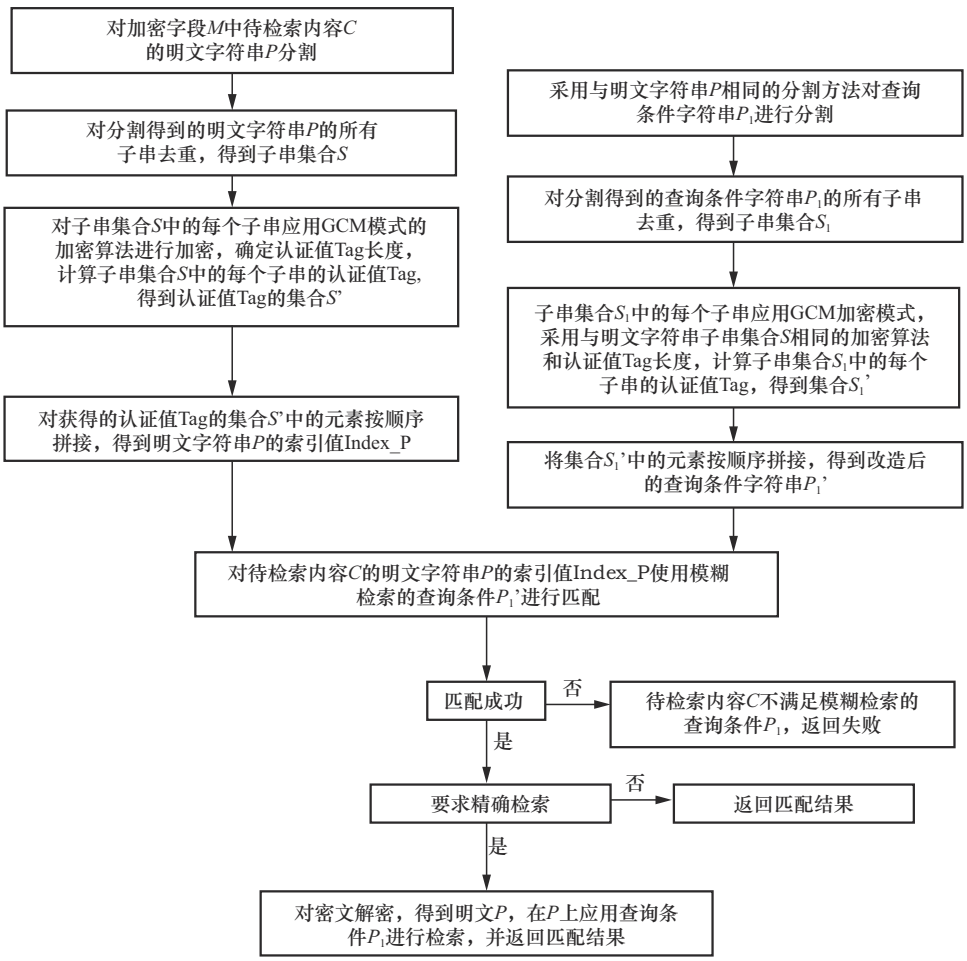

图14　密文模糊查询流程

（page）且每次只能锁定整页内存，被指定的区间涉及的每个内存页都将被锁定。内存清空机制在密钥使用结束时，强制将内存清空，以避免在内存上造成数据泄漏，定制的内存清空机制，保证了清空操作不会在编译的过程中被某些编译优化程序优化掉。

（2）落盘后的保护机制

在应用服务端，密钥工作时只存在于内存之中，并不存在需要落盘存储的密钥。根密钥只存在于密钥管理模块，在密管模块中，模块密钥需要进行落盘存储，使用根密钥加密后，以密文形式存储于数据库中，在使用的时候由根密钥进行解密，但解密后的模块密钥明文不会落盘。

2.5　技术方案比较

与传统的使用加密机加密的方案相比，本方案有明显的优势，传统的加密机加密需要在应用程序开发集成加密机的客户端SDK，量子数据库加密与传统数据库加密对比见表1。

3　结束语

本文提出的数据库加密方案，基于量子密码服务平台，所有根密钥和模块密钥均来源于量子安全服务平台中的量子随机数发生器件，随机数来源物理真随机，随机性来源于激光自发辐射光子的相位涨落，输出的随机数可通过国密、NIST等随机性测试。密钥来源的真随机是保证系统密钥管理体系安全可靠的底层基石。

表 1　量子数据库加密与传统数据库加密对比

比较项	量子数据库加密	传统加密方案
实施成本	无须改造应用功能代码，可快速实施	需要改造应用功能代码，集成加密机客户端 SDK，工作量大
部署方式	通过主路部署插件和旁路部署管理平台相结合的方式，不改变原数据流转路径和网络拓扑	等同于将加密机串联部署在主路中，改变了原数据流转路径，明文需要先经过集成的 SDK 传送到加密机，由加密机加密后再返回集成的 SDK 处，最终存入数据库
性能	基于高性能国密算法实现，对应用运行效率影响可忽略	需要将数据传入、传出加密机，额外增加了网络带宽和传输成本，并且受带宽和网络状态影响程度较大，从而使性能降低
可靠性	插件成为程序的一部分，不单独启动进程，插件的可靠性取决于应用自身的可靠性，可靠性高	数据需要传输给集中部署的加密机进行加/解密，形成性能瓶颈和单点故障风险，可靠性低
安全性	明文数据不会传出应用和数据库之外，安全性高	明文数据需要通过网络传输给加密机，有泄露和中断的风险
扩展性	可视化策略管理，配置或修改策略简单快捷，可方便进行加密字段的增加和减少，以及要保护应用的增加和减少	加密策略需要通过硬代码实现，任何策略改动，都需要改动代码，不灵活而且风险大
对应用影响	加/解密功能与应用系统轻耦合，不影响应用系统的升级迭代	加/解密与应用系统代码紧耦合，应用系统升级迭代需要考虑集成开发工作

并能提供“主体到数据库用户，客体到字段级”的细粒度身份访问控制。可通过数据安全管理方案对数据库访问者进行权限管理。在密文数据被访问时，则根据数据库访问者身份，向授权的用户展示明文数据或部分遮掩数据，而向未授权用户展示密文或脱敏数据。管理员可以通过设置加/解密和脱敏策略，对不同的数据库字段采用不同加密算法和密钥，实现敏感数据访问授权最小化。

本文提到的数据库加密做到了安全与合规两个维度，采用的高性能国密套件在保证了国密算法性能满足应用的同时，也实现了自主可控。遵循《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》的规定，方案中采用的密码模块（包括硬件与软件），均具备国家密码管理局颁发的商用密码产品认证证书，需要采用国密算法保护重要数据的机密性、完整性等。该标准中对于重要信息系统的密码应用做了明确规定，包括但不限于应用和数据安全以及密钥管理等方面。

量子密码服务平台将敏感数据在应用服务内加密，除了实现将数据加密后存入数据库，还能实现数据从应用服务到数据库之间以密文形式传输，因此，安全性更高，合规性更好。同时，在数据库的控制范畴内，不论是存储磁盘还是数据库范围内的内存、缓存，关键敏感信息是密文状态。

根据此次实际建设案例得出结论，当数据库需要做量子加密时也需要注意以下几点事项。

（1）量子数据库加密方案比较适用于加密冷数据（归档数据），如客户历年资料备份、身份证、手机号等。

（2）对数据库进行量子加密视情况需要更改表结构。

（3）加密会导致加密字段的数据量扩大 8 倍，如需要模糊查询，则要扩大 16 倍。

（4）Web 的框架需要使用 JAVA，Python 的框架不直接支持。

（5）操作数据库不能直接用 navicat，只支持 DBA。

（6）针对加密字段，若要使用并表查询，需要对涉及的字段均使用同一加密方式进行加密。

参考文献：

[1] 陈立佳, 刘菲, 史铭, 等. 基于量子的数据通信安全应用研究[J]. 财经界, 2016(5): 115-118.

[2] 彭鹏, 丁晓光. 基于量子保密通信技术的经典网络加密方案[J].

江苏通信, 2019, 35(3): 79-81.

[3] 王栋, 李国春, 俞学豪, 等. 基于量子保密通信的国产密码服务云平台建设思路[J]. 电信科学, 2018, 34(7): 171-178.

[4] 吕品, 苑涛. 量子计算云平台的应用生态建设和发展建议[J]. 信息通信技术与政策, 2024(7): 18-23.

[5] 罗俊, 刘驰, 王丙磊. 融合量子密钥分配的电信运营商密码应用体系[J]. 电信科学, 2023, 39(1): 136-145.

[作者简介]

陈云帆（1999– ），男，中国电信股份有限公司上海政企客户支撑响应中心/量子能力中心技术经理，主要研究方向为量子通信技术、5G技术、PON光网技术等。

蔡敏（1978– ），女，中国电信股份有限公司上海政企客户支撑响应中心/量子能力中心高级工程师，主要研究方向为量子通信技术、IP网络技术、5GtoB和物联网等。