基于服务器密码机的数据加密保护技术研究

王森
（国家信息中心 信息与网络安全部　北京市　100045）

摘　要：本文针对云环境下服务器密码机使用，详细介绍了云服务器密码机的模式、部署方式及应用要求。通过全面介绍基于服务器密码机的数据加密，为信息安全工作人员提供该领域技术参考。

关键词：服务器密码机；数据加密；对称加密算法 SM4；哈希算法 SM3

数据是重要的战略资源，做好数据安全的意义重大。数据安全涉及国家安全及高价值数字资产保护，同时数据管理面临篡改、窃取、破获等安全威胁，与拒绝服务攻击、漏洞攻击等网络攻击表现形式不同，数据安全事件破坏性不那么强烈，但导致的不良后果及负面影响巨大而且长远，重要数据泄露后便无法彻底清除回收，涉及敏感个人信息的数据泄露往往对现实生活安全产生影响。

数据保护面临的主要威胁源于恶意攻击者实施的数据窃取和篡改，数据泄露产生的不良后果和负面影响通常巨大并且长远。泄露的重要数据无法彻底清除回收，包括敏感个人信息的数据泄露往往会对人们现实生活安全产生影响。目前各方面在建设有效的数据安全保障体系方面开展了积极探索，数据安全保护的措施包括数据分类分级保护[1][2]、数据安全风险评估及监测预警[3]、数据安全应急处置[4]、数据安全审查[5]等方面方法，但相关技术标准和实施方案仍不成熟，各方面在建设有效的数据安全保障体系方面开展了积极探索。相较之下，采用密码保护是公认的最有效、最可靠、最经济的保障方案[6]，通过密码技术加密将保护数据加密成密文，即使发生数据泄露，敌手也无法还原出有意义的明文信息原文。

近年来制定实施的出台的多项网络安全政策文件、规范标准在对数据加密或数据保密性方面提出要求。《中华人民共和国网络安全法》（2017 年 6 月 1 日施行），对网络运行安全进行规范，提出“防止网络数据泄露或者被窃取、篡改”，应“采取数据分类、重要数据备份和加密等措施”（第二十一条）。《关键信息基础设施保护条例》中关于数据加密要求进行规范，“采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性”（第六条）。《个人信息保护法》中提出在个人信息处理过程中，应“采取相应的加密、去标识化等安全技术措施”（第五十一条）。《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》[7] 对于等级保护第三级及以上安全要求对象，在“安全计算环境”安全计算环境方面要求中“应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等”（位于 8.1.4.8 条）。《GB/T 41479-2022 信息安全技术 网络数据处理安全要求》[8] 在数据存储方面提出相关要求“存储重要数据和个人信息等敏感网络数据，应采用加密、安全存储、访问控制、安全审计等安全措施”（位于 5.3 条）。

使用密码对数据进行保护时，密码本身安全性同样应予以重视。因为只有密码技术只有得到合规、正确、有效应用，才能发挥支撑作用，乱用、误用密码技术，使用了不合规、不安全的密码产品会造成比不用密码技术更广泛、更严重的安全问题。为了规范密码应用和管理，《中华人民共和国密码法》制定实施。配套的密码技术标准和应用标准也在不断丰富完善，目前在密标委已制定 119 项密码行业标准，并通过网站进行发布[10]，多项已上升为国家标准，如《信息系统密码应用基本要求》信息系统密码应用基本要求、《密码模块安全要求》密码模块安全要求等。在使用密码进行技术实现数据安全保护过程中应充分遵从以上密码安全标准。

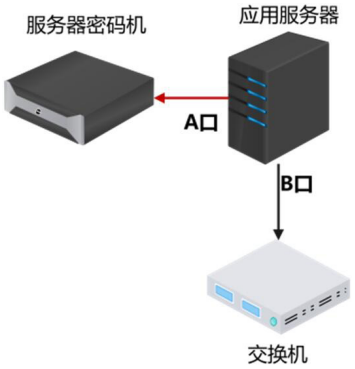
从数据安全需求入手，本文介绍了在我国现有规章制度和技术标准体系下的密码加密数据保护相关技术，完成了对相关实践总结。

1 基于服务器密码机的数据保护

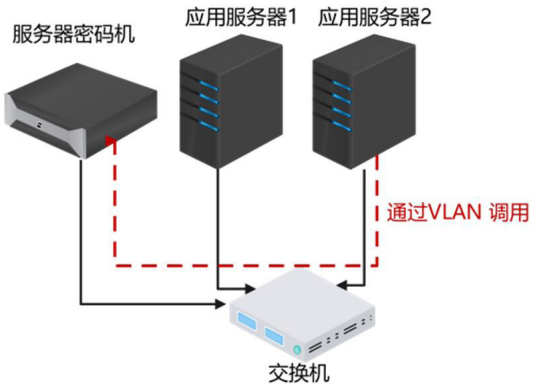
在信息系统应用安全中，一直重视采用加密技术进行防护。例如，在早期互联网应用登录中，数据库用 MD5 存储登录口令（password）的哈希值，用户登录认证时计算用户提交的口令 MD5 结果，比对数据库进行判断，当哈希值相等时完成身份认证判断。采用口令 MD5 方式，实际上保护了口令的明文，对数据泄露后数据保护具有一定的作用，但目前有很多攻击方法可以通过 MD5 值破解相应原文[11]，在现有密码管理政策中，使用 MD5 已经属于使用不合规的密码算法了。

针对数据库中大量的敏感信息，应该采用更安全的加密方案。《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》[12] 是开展信息系统建设应用密码技术的主要依据。目前有三种方式，一是存储在具有商用密码产品型号的加密硬盘中；二是存储在外部具有商用密码产品型号的存储加密设备中；三是利用外部服务器密码机加密后再进行存储[13]。第一种、第二种方式虽然使用比较最方便，数据加密存储和解密读取对应用都是“透明”的，不需要修改现有应用，但缺点也比较明显，价格较高不适用于低成本的应用场景。采用第三种部署服务器密码机的方式，需要在代码上进行调整，并且要改变原有拓扑结构。优势是价格相对便宜，方案比较成熟，数据加密由业务控制，可以防止防止数据库或存储管理员窃取数据等安全事件威胁发生。

图 1：某厂商密码机外观



(a) 直连模式



(b) 交换机连接

图 2：直连模式和交换机连接模式

在实践工作中，主要采用部署服务器密码机 [14]，通过在应用中调用服务器密码机的加 / 解密接口，将数据传递给密码机，获取计算结果后透传给数据库进行存储。

2 服务器密码机部署

服务器密码机是以整机形态出现，具备完整密码功能的产品，通常实现数据加解密、签名 / 验证、密钥管理、随机数生成等功能。（除服务器密码机外，还有链路密码机、签名验签密码机、金融密码机等 [15][16]，本文以下用密码机特指服务器密码机）。应用密码机满足了密码应用的多种安全性要求，一是密码机本身具有较高的安全性，自身能够抵御黑客远程控制或物理拆卸等攻击。二是密码机提供了符合政策标准要求的密码算法。三是密码机实现了安全的密钥管理，能够防止用户密钥泄漏。四是密码机是支持密码运算的特定部件，运算速度较高。目前我国服务器密码机运算速度能够满足应用需求，SM3、SM4 处理速率可达 10Gb/ 秒，SM2 签名速率可达 150 万次 / 秒。

密码机的硬件架构分成两类型。一是采用工控机 + 密码卡（PCI 接口），密码卡负责执行密钥管理和密码运算，在工控机上提供对外服务接口。另一类密码机采取自主设计芯片的技术路线，将密码芯片集成到计算机主板上。如图 1 所示，从外观上看密码机和普通服务器相似，可以放置在机房机架中。

2.1 密码机的部署方式

按照相关技术规范要求，通常密码机和应用服务器应采用直连方式，即应用服务器的一个网口与服务密码机服务网口连接（服务密码机通常具有多个服务网口及一个管理网口）。

如果不能满足应用服务器与密码机直连要求，在同一个机房中可以通过交换机设置 Vlan 或进行访问控制的方式，保护密码机访问。

有时密码机部署在安全管理区或密码设备管理区，这种分区划分便于统一进行访问控制，也可以实现密码设备和安全设备的集中管理。此时如果应用服务器和密码机采用跨区方式部署，必须采用通信信道保护。因为应用服务调用密码机服务时，需要将明文等信息传递至密码机进行运算，在通信信道上传递的数据是明文形式，如果通信不采用身份认证、加密等保护措施，系统将产生新的数据泄露风险点。密码机部署架构如图 2、图 3 所示。

2.2 密码机配置管理

应用服务器通过密码机厂商提供的配套驱动程序，设置密码机 IP 地址、认证口令等，配置成功后可以实现像本地函数一样的调用方式。

可以通过密码机的服务接口对其状态进行检查，密码机采用《GM/T 0018 密码设备应用接口规范》中设备状态结构体，返回的设备相关信息，结构体各字段如下所示。

```
typedef struct DeviceInfo_st{
    unsigned char IssuerName[40];  // 设备生产厂商名称
    unsigned char DeviceName[16];  // 设备型号
    unsigned char DeviceSerial[16]; // 设备编号，包括日期、批次号、流水号
    unsigned int DeviceVersion;    // 密码设备内部软件的编号
    unsigned int StandardVersion;  // 密码设备支持的接口规范版本号
    unsigned int AsymAlgAbility[2]; // 支持的非对称算法
    unsigned int SymAlgAbility;    // 支持的对称密码算法
    unsigned int HashAlgAbility;   // 支持的杂凑算法
```

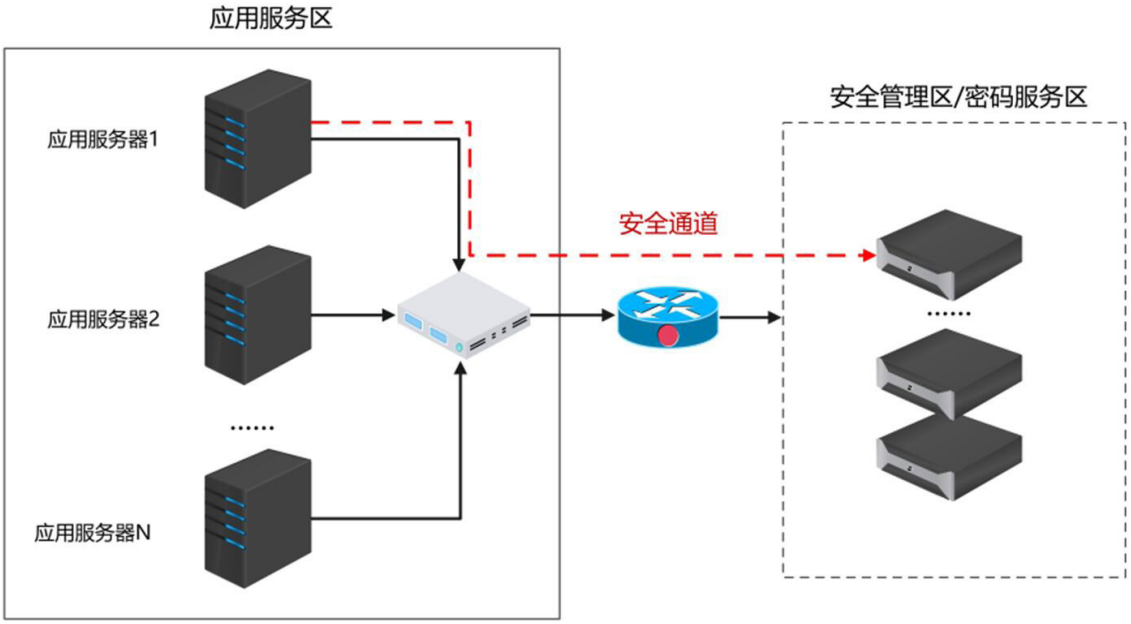


图 3：跨网段访问模式

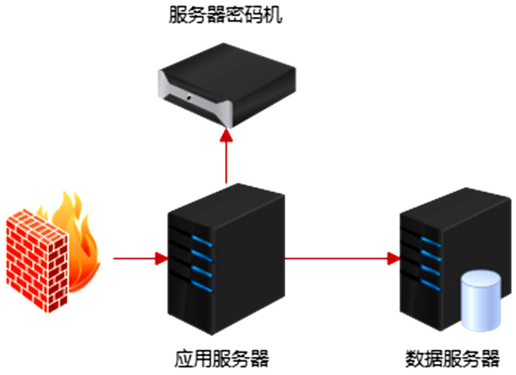


图 4：部署服务器密码机的系统架构图

unsigned int BufferSize; // 支持的最大文件存储空间（字节）

}DEVICEINFO;

为获取密码机支持的对称加密算法，详细介绍 SymAlgAbility 含义，该字段长度为 4 字节，该值代表为对称加密算法标识按位“或”运算结果。对称加密算法标识的编码规则为：从低位到高位，第 0 位到到第 7 位表示分组密码工作模式，第 8 位到第 31 位按位表示分组密码算法，例如：

SGD_SM1_ECB:0000 0000 0000 0000 0000 0001 0000 0001(0x00 00 01 01)

SGD_SM4_ECB:0000 0000 0000 0000 0000 0100 0000 0001(0x00 00 04 01)

SGD_SM4_CBC:0000 0000 0000 0000 0000 0100 0000 0010(0x00 00 04 02）、

国密对称加密算法包括 SM1、SSF33、SM4、ZUC，工作模式包括 ECB（ Electronic Code Book 电码本模式）、CBC（Cipher Block Chaining 密码分组链接模式）、CFB（Ciphertext Feedback 密文反馈模式）、OFB（Output Feedback 输出反馈模式）等[17]。ECB、CBC、CFB、OFB 的编码为 01、02、04、08。

2.3 密码机的调用

以典型 Web 应用将密文存储到数据库为例，系统结构如图 4 所示。密码机完成初始化后，进入就绪状态，应用服务器可以通过接口调用密码机服务。

2.3.1 数据加密

当应用中产生需要写入数据库的数据时，在调用数据库应用接口执行 Insert 命令前，调用密码机服务器的对称加密服务，根据密码设备接口标准[18]，对称加密函数名声明应为 SDF_Encrypt，并根据函数声明设置明文数据、密钥句柄等参数等，根据接口函数返回值，获得加密后的密文，并将密文存储到数据库中。当应用从数据库中读取数据时，应首先解密密文，密码设备解密函数的声明为 SDF_Decrypt。如图 5 所示。

服务器密码机的接口使用是一个有状态的过程，需要遵循一定的顺序，并且需要维持上下文，包括打开设备、创建会话、加密、关闭会话、关闭设备等流程，每个过程的函数声明和作用如下：

0. SDF_GenerateKeyWithKEK：创建加密密钥，获得加密密钥句柄；

1. SDF_OpenDevice: 打开设备，获得设备句柄；

2. SDF_OpenSession: 创建会话，获得会话句柄；

3. SDF_Encrypt: 利用会话密钥加密数据；

4. SDF_CloseSession: 关闭会话，销毁会话句柄；

5. SDF_CloseDevice: 关闭设备，销毁设备句柄。

创建加密的密钥，函数声明如下，

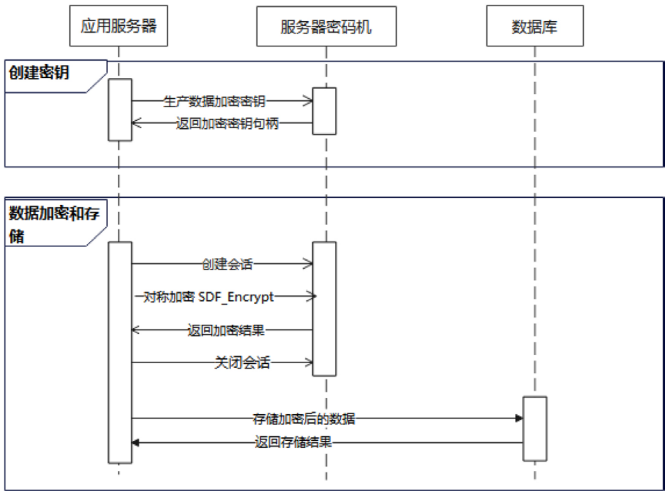


图 5：数据加密及存储到数据库流程

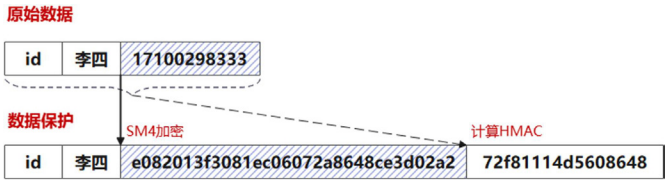


图 6：数据加密保护示例

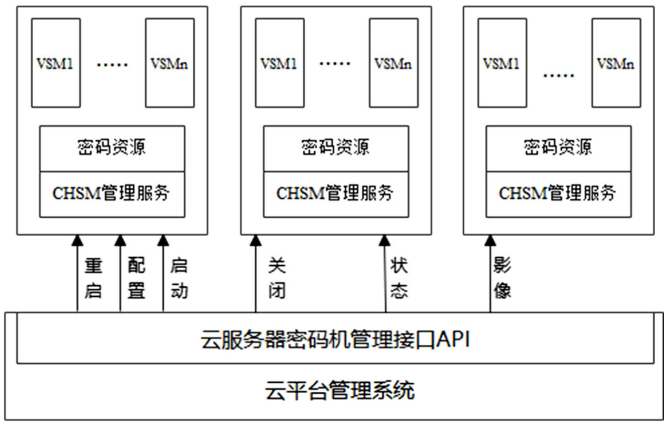


图 7：云服务器密码机系统架构

```
int SDF_GenerateKeyWithKEK(
    void * hSessionHandle,
    unsigned in uiKeyBits,
    unsigned int uiAlgID,
    unsigned int uiKEKIndex,
    unsigned char *pucKey,
    unsigned int *puiKeyLength,
    void **phKeyHandle);
```

uiKeyBits 指定生成加密密钥的长度，SM4[19] 需要密钥长度为 16 字节；uiAlgID 是算法标识，SM4 算法标识为 0x00 00 04 01[20]；uiKEKIndex 为密码机内部存储密钥加密密钥的索引值，加密密钥在密码机中必须不能以明文方式存储，因此在密码机中密钥的存储应采用相应的密钥加密密钥，加密后进行存储，密钥加密密钥 KEK 在采用索引方式引用；phKeyHandle 为返回的密钥句柄，应用于加密、解密函数。

2.3.2 完整性保护

完整性保护的目的是为了防止数据被篡改，因此数据的完整性保护与机密性保护同样重要。数据完整性保护机制是在数据存储时计算敏感数据的杂凑值，并一起保存在数据库中。读取数据库时获得数据后，应采用相同的哈希算法计算杂凑值，通过比较计算杂凑结果和数据存储时的杂凑值，当两值相同时可以证明数据记录没有被篡改。这里必须注意的是，如果攻击者能够修改存储数据，可以将数据和杂凑值一同修改，即替换修改后数据的杂凑值。因此，用于完整性保护时，杂凑算法与密钥一同使用，生产的杂凑值称为 MAC，这样的杂凑算法称为带密钥的杂凑算法（Keyed-hash Message Authentication Code，HMAC）[21]。采用 SM3 杂凑算法 [22]，密钥 K、消息 D，计算 HMAC 的公式如下：

$$HMAC_{SM3}(K,D) = H((\overline{K} \oplus OPAD) || H(\overline{K} \oplus IPAD) || D))$$

密码机计算 MAC 接口函数原型为

```
int SDF_CalculateMAC(
void * hSessionHandle,
void *hKeyHandle，
unsigned int uiAlgID，
unsigned char *pucIV,
unsigned char *pucData,
unsigned int uiDataLength,
unsigned char *pucMAC,
unsigned int *puiMACLength);
```

hSessionHandle 代表建立的密码机会话句柄，hKeyHandle 代表计算 HMAC 需要的密码句柄，uiAlgID 代表制定的 MAC 算法，SM3 算法标识为 SGD_SM3(0x00 00 00 01)，pucData 代表需要进行 MAC 计算的明文。

以如下的数据库模型为例，表设计为 (id, 姓名 , 手机号)，进行加密安全性保护之后表结构 (id, 姓名 , 加密 [手机号],MAC)。手机号涉及个人敏感信息，采用 SM4 加密保护，并将一条数据记录中字段拼接成整体计算 MAC，保存在字段 MAC 中。读取数据时，首先解密手机号，再拼接计算 MAC`，计算 MAC 与 MAC` 是否相等，判断记录的完整性是否被破坏。如图 6 所示。

3 云服务器密码机

随着大部分应用采用云的方式部署，部署独立的密码机问题越来越多。首先，在云环境下用户无法自行部署，密码机不能放在云服务的机房中；其次，云环境下服务器的拓扑结构超出了简单的架构，必须为了实体服务器做好网络上的访问控制，才能满足应用服务器和密码机之间的通信保护；第三，云环境下应用服务器数量多，对密码机数服务能力、运算速度、密钥管理数量等要求较高，使用独立的密码机管

理复杂度较大。

为了满足云环境下的密码机使用需求，云服务商与密码机设备厂商合作开发了云服务器密码机（cloud cryptographic server），可以在云计算环境下，采用虚拟化技术，以网络形式，能够为多个租户的应用系统提供密码服务的密码设备[24]。虚拟密码机（virtual cryptographic server）云服务器密码机上，采用虚拟化技术创建出来的提供类同实体密码机服务的密码服务实例。云服务器密码机和虚拟密码机由被称作 cloud-hosted hardware security module（CHSM）和 virtual security module（VSM）。

云服务器密码机提供了管理对接 API，并支持创建多个虚拟密码机，系统架构如图 7。从系统架构可以看出，将实体的密码机进行虚拟化后，使一台实体密码机能够提供多台独立服务的虚拟密码机（VSM），提高了密码机的使用效率。云平台通过 CHSM 的管理接口，并对底层硬件设备进行高度抽象，屏蔽了硬件差异，为上层应用提供统一服务[24][25]。

目前并不是所有的密码机都可以支持在云环境部署，并且能够进行云化部署的密码机，应符合《GM/T 0088-2020 云服务器密码机管理接口规范》。除公有云平台外，在政务云中建设云服务密码管理或云密码资源池，还应该遵守相关要求，一是云平台自身使用的密码资源池应当与供租户使用的密码资源池分开；二是一个密码资源池的服务范围最大为一个机房；三是基于云平台建设的基础设施安全支撑平台应当使用独立的密码资源池。以上密码机的资质及云平台密码资源池要求，应被作为云环境下密码安全性评估的重要要求。

4 结束语

近年来，数据加密存储越来越被重视，相较于只用哈希算法进行简单加密，应用中使用的算法强度、密钥管理、密码模块等方面及国产化适配性在更多政策文件、规范标准中提出要求。越来越多的应用场景按要求使用了服务器密码机，但是仍然存在没有使用、使用不规范等问题，存在只有机密性等级高的数据信息才需要使用密码机等认识偏差。本文从详细介绍了有关服务器密码机部署模式、调用方法、密钥管理等相关技术，并对云环境上服务器密码机的管理和使用详细进行了介绍，能够对应用系统中数据加密保护起到促进作用。

参考文献

[1] 高磊，赵章界，林野丽，翟志佳．基于《数据安全法》的数据分类分级方法研究 [J]．信息安全研究，2021，7(10)：933-940.
[2] 洪延青．国家安全视野中的数据分类分级保护 [J]．中国法律评论，2021(05)：71-78.
[3] 范絮妍，吴小倩，冯立胜，王欣．电子政务数据安全态势感知平台建设实践探索 [J]．信息安全研究，2021，7(10)：954-961.
[4] 高亚楠．电子政务数据安全治理框架研究 [J]．信息安全研究，2021，7(10)：962-968.
[5] 李政葳．筑牢数据安全防线 推进审查制度完善 [N]．光明日报，2022-02-19(003).
[6] 本刊编辑部．国家密码管理局局长李兆宗：新时代密码工作的坚强法律保障 [J]．中国信息安全，2019(11)：52-53.
[7] GB/T 22239-2019，信息安全技术 网络安全等级保护基本要求 [S].
[8] GB/T 41479-2022，信息安全技术 网络数据处理安全要求 [S].
[9] 百度百科．MD5[EB/OL]．[2022-6-27]．https://baike.baidu.com/item/MD5
[10] MD5 在线解密破解．CMD5．[EB/OL]．[2022-6-27]．https://www.cmd5.com/password.aspx
[11] 密码行业标准化技术委员会．标准查询．[EB/OL]．[2022-6-27]．http://www.gmbz.org.cn/main/bzlb.html
[12] GB/T 39786-2021，信息安全技术 信息系统密码应用基本要求 [S].
[13] 霍炜，郭启全，马原．商用密码应用与安全性评估 [M]．北京：中国工信出版社 / 电子工业出版社，2020
[14] GM/T 0030-2014，服务器密码机技术规范 [S].
[15] GM/T 0045-2016，金融数据密码机技术规范 [S].
[16] GM/T 0029-2014，签名验签服务器技术规范 [S].
[17] GB/T 17964-2021，信息安全技术 分组密码算法的工作模式 [S].
[18] GM/T 0018-2012，密码设备应用接口规范 [S].
[19] GB/T 32907-2016，信息安全技术 SM4 分组密码算法 [S].
[20] GB/T 33560-2017，信息安全技术 密码应用标识规范 [S].
[21] GB/T 15852.2-2012，信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制 [S].
[22] GB/T 32905-2016，信息安全技术 SM3 密码杂凑算法 [S].
[23] GM/T 0088-2020，云服务器密码机管理接口规范 [S].
[24] 华为技术有限公司．密钥管理服务用户指南 [EB/OL]．[2022-6-27]．https://static.huaweicloud.com/upload/files/pdf/20170901/20170901200948_55110.pdf.
[25] 阿里云．加密服务用户指南 [EB/OL]．[2022-6-27]．https://help.aliyun.com/product/28341.html.

作者简介

王森（1983-），男，辽宁省辽阳市人。计算机专业硕士。研究方向为电子政务、网络安全、密码应用、数据安全。