# 基于国密算法的航天数据保护方法研究与实践

杨继春[1] 王宏博[1] 吴广胜[2] 曹伟锋[2]
YANG Jichun WANG Hongbo WU Guangsheng CAO Weifeng

**摘 要** 为进一步探究并验证基于国密算法的航天数据保护方法的有效性与可行性。通过剖析航天数据保护的需求和应用现状，运用 SM4 加密算法开展性能优化和安全网络架构设计，进一步提升数据加密与传输过程的安全性。研究结果表明：优化 SM4 算法在显著提升加密处理效率的同时，优化网络安全方案对数据传输与存储也具有坚实的安全保障。结论显示，该研究中所提方法有效提高了航天数据安全防护水平，可为中国航天事业数据安全保障提供可靠技术支持。

**关键词** 国密算法；航天数据；数据保护方法

doi：10.3969/j.issn.1672-9528.2025.04.033

## 0 引言

在航天领域中，数据安全性至关重要。由于航天数据传输具有特殊性、高敏感性等特点，常规数据保护方法很难适应其复杂多变的安全要求。国密算法是我国自行研制的高强度加密技术之一，为航天数据保护问题提供了一种新型解决方案[1]。所以，对基于国密算法航天数据保护方法进行研究与实践，既有利于促进我国航天领域数据安全水平的提高，又能够促进相关技术的创新与应用，因而具有一定的理论意义与现实意义。

## 1 应用现状

### 1.1 物理和环境安全

航天测控综合管理系统中物理设备储存于机房中，有可能会受到机房非法侵入、门禁系统记录篡改以及监控视频数据损坏等问题。这些物理安全问题会造成系统设备直接损坏或数据泄露。

### 1.2 网络和通信安全

航天测控综合管理系统的数据传输没有使用密码技术加以防护，存在身份数据被非法截取、伪造以及在数据传输阶段遭到篡改的潜在危险。

### 1.3 设备和计算环境安全

各个操作终端与应用设备之间的身份鉴别机制并没有采用密码技术而依赖于容易破译的口令，这可能会造成对服务器的侵入以及对设备鉴别信息的篡改，从而对系统安全构成威胁。

### 1.4 应用和数据安全

系统数据库、配置数据、日志数据及其他敏感信息未使用加密存储技术易造成重要数据被盗用，极大地影响了系统中数据的机密性与完整性。总之，TDCS/CTC 系统中密码技术的应用存在着明显的缺陷，急需强化安全保障措施来提升整体的安全性。

## 2 需求分析

### 2.1 网络架构

航天测控综合管理系统包括站点中心局域网，站点局域网和广域网，其网络架构是否合理直接关系到业务承载能力的大小。应用密码技术需要满足网络设备冗余，传输通道冗余和路由冗余，保证数据传输可靠稳定。

### 2.2 通信传输

航天测控综合管理系统是一个需要加强对业务通信数据的防护的专用系统，对重要的数据可以使用安全的通信协议进行处理。需要保证信息传输与存储时内容一致，为篡改攻击检测与发现提供机制，从而达到通信过程完整与保密。

### 2.3 可信验证

为了抵抗恶意攻击，可以在数据传输时利用探针技术深度解析通信数据，避免恶意用户假冒合法业务数据或者篡改传输路径等行为，保证数据传输真实安全。

## 3 SM4 加密算法性能优化

### 3.1 SM4 轮密钥缓存

透明的加密方法，在实际应用中，高频的加密和解密操作可能会对系统性能产生影响。例如，当需要对大量数据的数据库进行全面加密时，系统会调用基础的 SM4 加密接口：

cipher = SM4Enc(key, plain)

密码接口的需求是将 128 bit 的 SM4 加密密钥转化为 32 个 32 bit 的轮密钥。由于轮转密钥与轮密钥之间存在一一对应关系，因此每次更新轮密钥时必须重新初始化整个系统。

1. 西安寰宇卫星测控与数据应用有限公司 陕西西安 646099
2. 陕西省数字证书认证中心股份有限公司 陕西西安 710075

频繁地使用同一接口并使用相同的密钥进行加密会消耗大量的时间，通过加密密钥 key 重复产生相同的轮密钥 rk，从而降低小数据包的整体加密和解密吞吐性能。因此本文提出一种基于轮盘赌和随机置换的密文转明文算法，在保证安全性基础上提高了大数据包传输效率。调整密码的接口设置为：

ctx=SM4SetKey(key)

cipher=SM4Enc(ctx,plain)

该应用程序能够预先调用 SM4SetKey 接口，将加密密钥输入到密码模块中，然后密码模块会将加密密钥转换为轮密钥，并保存在接口的上下文 ctx 里 [2]。在需要用相同的加密密钥 key 进行加密的情况下，系统会调用 SM4Enc 接口来输入上下文 ctx，并使用已保存的轮密钥进行加密和解密操作，这样可以跳过多次重复生成轮密钥的步骤，从而优化加密流程并提高 SM4-GCM 算法的性能 [3]。通过在不同硬件环境下对算法性能测试分析可知，本文提出的方法能够满足实际应用需求，且具有较高的安全性和效率，如图 1 和表 1 所示。

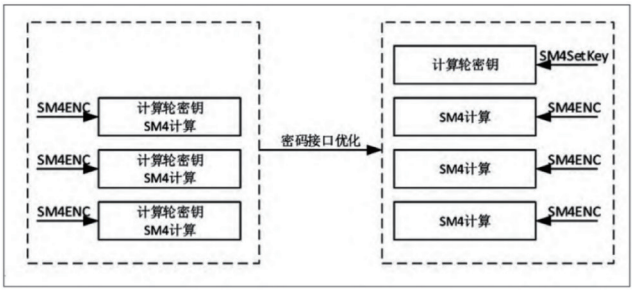


图 1 密码接口优化前后调用示意图

表 1 数据加解密普通加解密与轮密钥缓存方式性能比较情况

| 16 字节 | 普通 / (Mbit·s$^{-1}$) | 轮密钥缓存 / (Mbit·s$^{-1}$) | 性能提升 |
|---|---|---|---|
| 执行 500 000 次 | 234.96 | 1 008.00 | 329% |

3.2 指令层优化 SM4

基于标准 C 代码实现的 SM4-GCM 算法，可以利用处理器的指令来优化 SM4 算法。例如，在 x86 架构上使用特定的处理器指令，或者在使用兆芯 GMI、鲲鹏 KAE 等信创平台指令的 SDK 环境中直接调用 SDK 进行性能优化。本文还提出了一种新的循环移位寄存器结构，该结构能够降低循环移位寄存器的计算复杂度和存储空间占用。SM4 算法中的轮函数的非线性变化是依赖于 S 盒查表操作的，这些操作通常比较耗时，因此优化 S 盒查表过程可以显著提升 SM4 算法的运行效率 [4]。SM4 和 AES 的 S 盒都是基于有限域 GF（2^8）构建的，并且是通过逆运算和仿射变换来生成的。S 盒的具体生成步骤包括通过固定的置换方法将输入的 8 位二进制数打乱，接着将其代入一个由仿射变换和逆运算构成的函数中，从而最终确定输出的 8 位二进制数。该方法是一种特殊形式的循环移位型映射，其运算量比传统的线性矩阵求逆计算量少得多。这一生成方法采用了在有限域中的不可约多项式转换技术，从而使得 AES 和 SM4 的 S 盒能够在有限域内完成变换操作。因此，通过对 AES 和 SM4 的 S 盒特性的深入分析和应用，能够进一步完善 S 盒的查表流程，如图 2 所示。

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0a | 0b | 0c | 0d | 0e | 0f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 10 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 20 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 30 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 40 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 50 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 60 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 70 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 80 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 90 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a0 | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b0 | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c0 | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d0 | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e0 | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f0 | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

图 2 AES 算法的 S 盒

AES 算法的 S 盒定义在 GF（2^8）有限域的不可约多项式为：

$$x_8+x_4+x_3+x+1 \tag{1}$$

表达式为：

$$S(x)=Ax\text{-}1+c \tag{2}$$

ES 算法 GF（2^8）有限域不可约多项式矩阵计算方式为：

$$\begin{pmatrix} s_7 \\ s_6 \\ s_5 \\ s_4 \\ s_3 \\ s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{3}$$

SM4 算法的 S 盒定义如图 3 所示。

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | D6 | 90 | E9 | FE | CC | E1 | 3D | B7 | 16 | B6 | 14 | C2 | 28 | FB | 2C | 05 |
| 1 | 2B | 67 | 9A | 76 | 2A | BE | 04 | C3 | AA | 44 | 13 | 26 | 49 | 86 | 06 | 99 |
| 2 | 9C | 42 | 50 | F4 | 91 | EF | 98 | 7A | 33 | 54 | 0B | 43 | ED | CF | AC | 62 |
| 3 | E4 | B3 | 1C | A9 | C9 | 08 | E8 | 95 | 80 | DF | 94 | FA | 75 | 8F | 3F | A6 |
| 4 | 47 | 07 | A7 | FC | F3 | 73 | 17 | BA | 83 | 59 | 3C | 19 | E6 | 85 | 4F | A8 |
| 5 | 68 | 6B | 81 | B2 | 71 | 64 | DA | 8B | F8 | EB | 0F | 4B | 70 | 56 | 9D | 35 |
| 6 | 1E | 24 | 0E | 5E | 63 | 58 | D1 | A2 | 25 | 22 | 7C | 3B | 01 | 21 | 78 | 87 |
| 7 | D4 | 00 | 46 | 57 | 9F | D3 | 27 | 52 | 4C | 36 | 02 | E7 | A0 | C4 | C8 | 9E |
| 8 | EA | BF | 8A | D2 | 40 | C7 | 38 | B5 | A3 | F7 | F2 | CE | F9 | 61 | 15 | A1 |
| 9 | E0 | AE | 5D | A4 | 9B | 34 | 1A | 55 | AD | 93 | 32 | 30 | F5 | 8C | B1 | E3 |
| A | 1D | F6 | E2 | 2E | 82 | 66 | CA | 60 | C0 | 29 | 23 | AB | 0D | 53 | 4E | 6F |
| B | D5 | DB | 37 | 45 | DE | FD | 8E | 2F | 03 | FF | 6A | 72 | 6D | 6C | 5B | 51 |
| C | 8D | 1B | AF | 92 | BB | DD | BC | 7F | 11 | D9 | 5C | 41 | 1F | 10 | 5A | D8 |
| D | 0A | C1 | 31 | 88 | A5 | CD | 7B | BD | 2D | 74 | D0 | 12 | B8 | E5 | B4 | B0 |
| E | 89 | 69 | 97 | 4A | 0C | 96 | 77 | 7E | 65 | B9 | F1 | 09 | C5 | 6E | C6 | 84 |
| F | 18 | F0 | 7D | EC | 3A | DC | 4D | 20 | 79 | EE | 5F | 3E | D7 | CB | 39 | 48 |

图 3 SM4 算法的 S 盒

SM4 算法的 S 盒定义在 GF（2^8）有限域的不可约多项式为：

$$x_8+x_7+x_6+x_5+x_4+x_2+1 \tag{4}$$

生成方式为：

$$S(x)=A(Ax+c)\text{-}1+c \tag{5}$$

其中 SM4 算法 GF($2^8$) 有限域不可约多项式矩阵参数为：

$$A=\begin{pmatrix}1&1&0&1&0&0&1&1\\1&1&1&0&1&0&0&1\\1&1&1&1&0&1&0&0\\0&1&1&1&1&0&1&0\\0&0&1&1&1&1&0&1\\1&0&0&1&1&1&1&0\\0&1&0&0&1&1&1&1\\1&0&1&0&0&1&1&1\end{pmatrix},c=\begin{pmatrix}1\\1\\0\\1\\0\\0\\1\\1\end{pmatrix} \tag{6}$$

可以看到，SM4 算法和 AES 算法采用的有限域不可约多项式有所不同。SM4 算法采用的有限域不可约多项式为 $x_8+x_6+x_5+x+1$，生成方式为：

$$S_s(x)=A_s\cdot I_s(A_sx+C_s)+C_s \tag{7}$$

AES 算法采用的有限域不可约多项式为 $x_8+x_4+x_3+x+1$，生成方式为：

$$S_a(x)=A_a\cdot I_a(x)+C_a \tag{8}$$

在上述的数学表达式里，计算 $I_s$ 和 $I_a$ 的逆运算被认为是最为复杂和耗时的操作。可以设计一个同构映射 $T$ 来将 SM4 相关的有限域元素映射到 AES 相关的有限域元素上，然后利用指令进行求逆操作，最终实现逆映射。该方法可用于求解任意阶奇偶模对称矩阵方程或方程组。图 4 展示了 AES 和 SM4 的 S 盒同构映射操作。

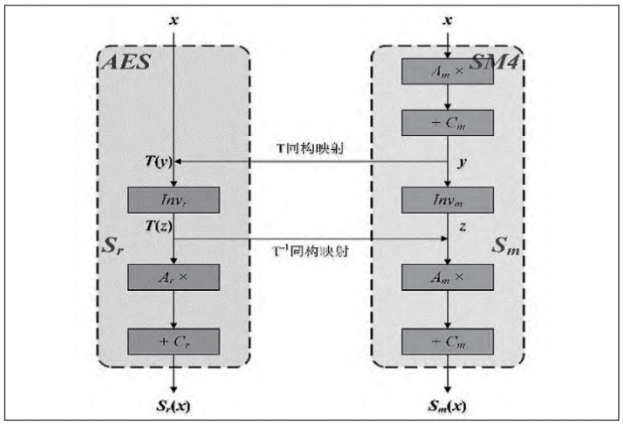


图 4 AES 和 SM4 的 S 盒同构映射运算示意图

记为：

$$y=A_sx+C_s \tag{9}$$

由 SM4 有限域映射到 AES 有限域的函数为 $T(x_s)\rightarrow x_a$。则 SM4 算法有限域求逆为：

$$\begin{aligned}I_s(y)&=T\text{-}1A_a\text{-}1\cdot\{S_a(T(y))+C_a\}\\&=T\text{-}1A_a\text{-}1S_a(T(y))+T\text{-}1A_a\text{-}1C_a\end{aligned} \tag{10}$$

将 $I_s(y)$ 代入 $S_s(x)=A_s\cdot I_s(A_sx+C_s)+C_s$，那么 SM4 算法 S 盒计算方式为：

$$\begin{aligned}S_s(x)&=A_sT\text{-}1A_a\text{-}1\cdot S_a(T(y))+A_sT\text{-}1A_a\text{-}1C_a+C_s\\&=\{A_sT\text{-}1A_a\text{-}1\}\cdot S_a(\{TA_s\}x+\{TC_s\})+\{A_sT\text{-}1A_a\text{-}1C_a+C_s\}\end{aligned} \tag{11}$$

经过深入分析得出结论：SM4 算法中的 S 盒运算可以通过求逆和映射等手段，转化为 AES 的 S 盒计算方法。这就使得该方法对硬件实现有很大帮助。在 x86 架构的 AVX2 指令集中，AES-NI 指令提供了硬件加速的 AES S 盒计算功能，能够在一个时钟周期内完成输入字节到输出字节的转换 [5]。由于该指令集支持多种密码技术，其实现过程也更加复杂。因此，为了加快 SM4 算法的 S 盒运算速度，可以采用 AES-NI 指令，尤其是 AESENCLAST 指令。同时也对该算法进行了性能测试。为适应 AESENCLAST 指令中的行移位和子密钥异或操作，通过调序指令来消除行移位，并将子密钥设置为全 0，从而消除异或的影响 [6]。实验结果表明，该方案不仅能够保证较高的处理速度，而且还具有良好的可扩展性。为最大限度地利用 AES-NI 指令的 128 bit 数据处理能力，采用 SMID 指令将 4 组 32 bit 的 SM4 消息整合到 128 bit 中，从而显著提高了 SM4 算法的运行效率。

打包操作过程如下：

（1）在 4 个 128 位寄存器的较低位置，分别保存了 4 个 32 位的整数。

（2）针对每一个寄存器，分别从其低 16 位和高 16 位中提取出两个 16 位的整数。

（3）对这两个 16 位的整数，进行了饱和转换，也就是将超出 16 位的数值进行截断。

（4）将经过饱和转换的 4 个 16 位整数融合为一个 128 位的数据块，并将此数据返回。

举例来说，如果输入的四个 32 位整数分别是 0x0000FFFF、0x00000000、0x00008000、0x00007FFF，那么打包后得到的 128 位数据将会是 0xFFFF0000FF0000000080007FFF。这也就是为什么打包后的数据量会比之前减少了一半。SMID 的数据打包功能能够把多个标量数据整合为一个更庞大的向量。由于不同大小的数据压缩后产生的长度也不一样，所以会出现较大的误差，这可能导致对同一文件或同样内容的操作结果存在差异 [7]。计算机处理芯片在执行一个小向量数据和一个大向量数据时，其时间周期是一致的。这是因为在进行分组时，每一组内的所有字节都会被计算出相应的值。因此，把 4 组 32 bitSM4 的消息转化为 SMID 向量，有助于加快计算的速度。在该变换中采用了一种新方法——组合法，即对

所有分组分别进行计算和比较后再合并。图 5 展示了结合 S 盒转换、AES-NI 指令和 SMID 指令的 SM4 算法的运算流程。

```
1.SM4ENC(M, K, M`)                  //SM4 加密函数，M 明文、K 轮密钥、M` 密文
2.M=M0,M1,M2,M3                     // 输入 128bit 消息，分为 4 组 32bit 的数据
3.X0,X1,X2,X3=M0,M1,M2,M3           // 将消息数据分组打包到寄存器
4.for i=0–>31                       // 执行 32 次轮函数
5.S=X1 ⊕ X2 ⊕ X3 ⊕ Ki               // 后 3 块消息与当前轮密钥进行异或
6.S=TA × S+TC                       // 转换 S 盒数据
7.S=Sa(S)                           // 通过 AESENCLAST 指令执行 S 盒运算
8.S=AT A × S+AT AC                  // 转换 S 盒数据
9.S=X0 ⊕ L(S)                       // 将结果与第一块消息数据进行非线性变换
10.X0,X1,X2,X3= X1,X2,X3,S          // 更新寄存器数据
11.M`=X0,X1,X2,X3                   // 寄存器数据分组解包到密文并输出
```

图 5 运算流程

x86 平台 SM4 算法性能比较情况如表 2 所示。

表 2 算法性能比较表

| 1 线程 1GB | 普通 / (Mbit·s$^{-1}$) | x64 指令优化 / (Mbit·s$^{-1}$) | 性能提升 |
|---|---|---|---|
| 执行 5 次 | 1 099.25 | 3 351.42 | 205% |

## 4 网络安全方案

航天综合视频监测系统的传输方法主要是基于国密算法而设计的数据加密方式，其整个加密技术是按照三级等保安全设计技术规范。整个安全方案主要涉及 3 个核心部分，即：安全计算环境、安全管理中心、边界保护区，由此构建一个基于国密算法的航天综合视频监控系统网络安全方案，具体架构如图 6 所示。

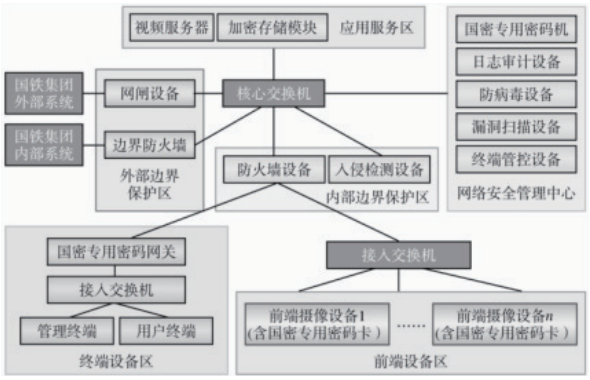


图 6 基于国密算法的航天综合视频监控系统网络安全方案

### 4.1 网络安全管理中心

网络安全管理中心的主要工作是保障航天综合视频监控系统的安全、稳定，其中心主要设备与功能如下所述：

（1）国密专用密码机：对于国家秘密数据、敏感数据进行加密处理，可以保证这些数据资料在传输过程中被安全拦截，尤其是可以杜绝这些数据被未授权用户读取。为了进一步规避敏感信息的外泄及提高数据的保密性，在加密研究中特别加入了完整的检查机制，这样可以有效避免数据传输中不会被恶意损坏或篡改 [8]。

（2）日志审计设备：此设备主要功能是监控、分析、记录系统、网络设备及应用程序所产生的日志数据，并进行综合管理。随着信息化技术的不断发展，企业在发展过程中对于数据信息的收集、处理能力有了更高的标准和要求。本方案在设计过程中尤其注重系统的安全性、合规性及运营效率，其可以快速识别网络传输中的安全风险或隐患、异常操作。

（3）防病毒设备：该设备的作用是预防计算机系统不会被网络恶意软件或程序损害，其主要工作是实时监控计算机病毒、检测网络潜在威胁、自动化隔离或清除，并实时更新安全规则库。

（4）漏洞检测设备：该设备可以实现周期性检查监控系统，并对存在的系统漏洞进行评估，从而及时、高效地发现并修复系统存在的网络安全漏洞，从而提高监控系统的网络安全性，并可以缩短病毒存在时间。

（5）终端控制设备：该设备运用白名单机制，针对外部或非法网络设备接入进行高效管理，以此确保整个监控系统设备可以安全、合法运行，预防外部设备非法入侵的可能性。

### 4.2 边界保护区

航天综合监控视频系统中的边界防护，其主要分为外部、内部，主要网络安全工具的功能阐述如下：

（1）防火墙设备：防火墙作为系统网络安全的主要设备，其具备有效隔离系统内部、外部网络，从而阻止内外部未被授权的数据泄漏或访问行为。

（2）入侵检测装置：该系统可以实现对网络流量的实时追踪，且快速、准确识别、分析可能存在的入侵行为，例如：病毒传播、网络入侵等。全方位地检查和评价网络是确保网络稳定运作的核心要素之一。当系统侦测到不正常的状况时，它会迅速发出预警，并采取必要的保护手段，确保网络的安全性得到充分的预警和维护。

（3）网闸设备：为了确保内部网络不会受到外部威胁，采纳了物理隔离技术，以实现网络的完全隔离和数据交换的严格控制 [9]。这项技术确保了内部网络和外部网络能够完全隔离，从而有效地避免了可能的恶意攻击和数据泄露。在为航天行业的各个单位实施安全防护措施时，必须深入考虑航天综合视频监控系统对信息安全管理的独特需求，并采纳实际且高效的安全预防方法，以确保航天综合视频监控系统能

够安全且稳定地工作。在航天综合视频监控系统的框架内，无论是内部还是外部的边界保护区，都实施了一系列主要的网络安全保护措施。

4.2.1 内部边界保护区

这片区域主要被划分为两个分界线：一个是应用服务区与终端设备的分界（被称为边界 1），而另一个则是应用服务区与前端设备的分界（被称为边界 2）。为了确保边界 1 和边界 2 的用户访问控制安全，并有效抵抗网络侵入，内部边界保护区采用了防火墙和入侵检测设备，这成为了边界防护的首要防线 [10]。

4.2.2 外部边界保护区

这片地域主要被划分为两个边界：一个是该系统与航空集团的内部系统之间的交叉点（被称为边界 3），另一个是该系统与航空集团的外部系统之间的交叉点（被称为边界 4）。其中边界 3 中的访问管理工作主要是运用边界防火墙技术，这样可以保证系统访问与数据共享过程中的安全性；边界 4 中的访问管理则是采用网闸设备进行管理，其中数据交换工作则是参考数据摆渡基准，通过这种方式可以有效避免监控系统被外部系统入侵的可能性。

4.3 安全计算环境

航天综合视频监控系统的安全计算环境主要分为 8 个方面，具体如下：

（1）数据加密存储：为了保证系统内的数据存储安全性，系统设计时在应用服务区专门增设了专为国密设计的数据加密储模块。

（2）加固操作系统：系统会定期自动更新操作系统补丁，同时及时关闭部分非必要端口或者服务，从而缩小被攻击范围。

（3）访问权管理：在执行角色访问控制策略过程中，可以保证用户可以获取最基本的资源访问权限，以保障完成相关任务。

（4）日志审查：激活系统内的日志，并使用日志审查工具实现定期审查，对异常行为进行监控，且可追踪安全事故发生。

（5）代码检查：定期对系统的应用程序代码进行检查、升级后，可以及时发现程序漏洞，并修改存在的安全隐患问题。

（6）渗透检测：系统可定期实施渗透测试，验证并清理所有输入的数据信息资源，预防可能存在安全隐患（如：预防注入攻击等）。

（7）数据备份：定期制定并执行数据备份计划，可保障系统数据资料被损坏后具备恢复功能。

（8）为了应对可能出现的灾害性事件，已经制定了详细的灾害恢复计划，并定期进行模拟训练。

## 5 结论

本次研究针对以国密算法为核心的航天数据保护方法，进行深入探究与实践应用，证明国密算法对于增强航天数据安全性是有效可行的。研究结果表明：通过合理设计网络架构，对通信传输进行安全加固和实施可信验证机制可显著提高航天数据安全保障能力。另外 SM4 加密算法性能优化与网络安全方案改进进一步提高数据保护整体效率与可靠性。该研究对今后航天领域数据安全问题提供一条切实可行的技术路径与实践借鉴，有利于促进我国航天事业安全持续发展。

**参考文献：**

[1] 李恒 . 基于高性能国密算法的数据库透明加密技术研究 [J]. 中国新通信 , 2024,26(18):24-28.

[2] 周由胜 , 丁珊 , 左祥建 , 等 . 一种基于国密算法的保密多方字符串排序协议 [J]. 电子与信息学报 ,2024,46(9):3763-3770.

[3] 王明登 , 严迎建 , 郭朋飞 , 等 . 基于 RISC-V 指令扩展方式的国密算法 SM2、SM3 和 SM4 的高效实现 [J]. 电子学报 , 2024, 52(8):2850-2865.

[4] 王作广 , 李超 , 赵利 . 基于零信任的网络数据安全保护框架与实现 [J/OL]. 计算机应用 ,1-12[2024-11-14].http://kns.cnki.net/kcms/detail/51.1307.TP.20240802.1325.004.html.

[5] 鲍婧 , 林炜峰 , 王学理 . 基于集成平台的互联网医院数据加密传输方案设计与实现 [J]. 中国数字医学 ,2024,19(7):97-101.

[6] 李春铎 , 杨轶杰 , 屈毅 . 国密算法在 5G-R 系统中的应用研究 [J/OL]. 铁道通信信号 ,1-10[2024-11-14].http://kns.cnki.net/kcms/detail/11.1975.U.20240524.1541.002.html.

[7] 高汉军 . 基于国密算法的工控系统组态程序隐私保护方案 [J]. 电子技术应用 , 2024(S1): 31-33.

[8] 王晶宇 , 马兆丰 , 徐单恒 , 等 . 支持国密算法的区块链交易数据隐私保护方案 [J]. 信息网络安全 , 2023, 23(3):84-95.

[9] DING H Y, MENG Q Q, SUN L H, et al.Design and implementation of microservice secure communication framework based on national secret algorithm and dynamic key[J].Journal of physics: conference series, 2022, 2384: 012048.

[10] 陈康 , 陆君一 , 沈尧 , 等 . 计价器强检中应用数据保护技术 [J]. 上海计量测试 ,2021,48(5):51-53.

**【作者简介】**

杨继春（1972—），男，陕西渭南人，硕士研究生，高级工程师，研究方向：航天测控。

（收稿日期：2024-12-03）