|  |
| --- |
|  |
| XXXX研制方案 |
|  |
|  |
| XXXX单位 |
| 二○XX年XX月 |

目录

[XXXX研制方案 4](#_Toc452043530)

[1 概述 4](#_Toc452043531)

[1.1 研制背景 4](#_Toc452043532)

[1.2 任务来源和依据 4](#_Toc452043533)

[1.3 研制目标 4](#_Toc452043534)

[2 主要功能与技术指标 4](#_Toc452043535)

[2.1 主要功能 4](#_Toc452043536)

[2.2 技术指标 4](#_Toc452043537)

[3 方案设计 4](#_Toc452043538)

[3.1 系统结构及组成 4](#_Toc452043539)

[3.2 工作原理 5](#_Toc452043540)

[3.3 硬件设计 5](#_Toc452043541)

[3.4 软件设计 5](#_Toc452043542)

[3.5 协议设计 5](#_Toc452043543)

[3.6 系统接口与信息交换关系（可选） 5](#_Toc452043544)

[4 密码密钥配用 6](#_Toc452043545)

[4.1 安全保护及管理保障需求分析 6](#_Toc452043546)

[4.2 密码配用（密码产品或模块请分别参考对应模板） 7](#_Toc452043547)

[4.3 密钥配用 7](#_Toc452043548)

[4.4 密码协议 8](#_Toc452043549)

[5 安全保密措施设计 9](#_Toc452043550)

[5.1 密码资源保护机制 9](#_Toc452043551)

[5.2 故障诊断和处置机制 10](#_Toc452043552)

[5.3 逻辑安全防护机制 10](#_Toc452043553)

[5.4 物理安全防护机制 10](#_Toc452043554)

[5.5 前向安全防护机制 10](#_Toc452043555)

[6 电子元器件国产化应用 10](#_Toc452043556)

[7 通用性设计 10](#_Toc452043557)

[7.1. 可靠性设计 11](#_Toc452043558)

[7.2. 维修性设计 11](#_Toc452043559)

[7.3. 保障性设计 11](#_Toc452043560)

[7.4. 安全性设计 11](#_Toc452043561)

[7.5. 测试性设计 11](#_Toc452043562)

[7.6. 环境适应性设计 11](#_Toc452043563)

[8 质量控制与标准化管理 11](#_Toc452043564)

[8.1. 质量控制要求 11](#_Toc452043565)

[8.2. 标准化管理要求 11](#_Toc452043566)

[9 关键技术分析 12](#_Toc452043567)

[10 任务分工 12](#_Toc452043568)

[11 进度安排 12](#_Toc452043569)

XXXX研制方案

# 概述

## 研制背景

重点从军事需求、装备发展、技术升级、应用要求等方面，简要分析、阐述项目的研制背景。

## 任务来源和依据

描述项目的研制计划或任务批复等，如为自拟项目，可省略。

## 研制目标

从满足使用需求、提升功能性能、提高技术水平等方面出发，确立研制目标。

# 主要功能与技术指标

## 主要功能

主要描述系统（设备）可实现的主要功能。

## 技术指标

描述系统（设备）应达到或满足的各项具体指标。

# 方案设计

## 系统结构及组成

阐述该项目所依托的信息系统、武器平台，给出相应的背景情况，包括使用环境、应用范围（部署地点）、功能用途，组织运用基本模式等。

结合密码系统（设备）在信息系统、武器平台中的配置方式，阐述密码系统（设备）的典型配置模式，并给出典型配置拓扑图，拓扑图应能体现信息的处理流程、装备的配置位置、以及对信息的处理方式和层次。

如为升级改造项目，要描述升级或改造的内容，并对原系统（设备）进行简要介绍。

## 工作原理

以流程图的形式描述密码系统（设备）工作的基本原理，采用图文相结合的方式描述。

## 硬件设计

描述系统（设备）硬件组成，分别说明各硬件模块设计方案，尽可能细化到功能部件。

对于应用于指控系统、武器平台、密码管理等的系统（设备），在功能性能和技术指标可满足的情况下，应优先选用《军队公用普通密码算法芯片选型指南》、《公用普通密码应用领域基础支撑产品简介》中发布的密码芯片（模块）或国产化芯片。

噪声源芯片必须使用《军队公用普通密码算法芯片选型指南》中推荐的产品。

## 软件设计

描述系统（设备）软件组成，分别说明各软件模块设计方案，尽可能细化到功能模块。

## 协议设计

描述系统（设备）的协议设计方案。

## 系统接口与信息交换关系（可选）

分别描述系统或设备的外部接口以及各分系统之间的内部接口关系，密码系统（设备）与外部（宿主）信息系统和密码系统内部的信息交互关系，一般包括信息交换需求与接口对应关系，可以按表格或图示方式体现外部和内部关系。

# 密码密钥配用

## 安全保护及管理保障需求分析

### 用户安全需求分析

采用文字和拓扑图相结合的方式阐述信息处理和保护的全过程（信息的来源和去向、密码处理层次等）。

根据应用环境，结合处理的信息类型，信息处理流程，承载信息的信道和网络等内容，分析可能面临的安全威胁以及潜在的攻击类型，给出用户信息的保护需求。

如果是密码管理系统（装备），则须按照上述要求，分析管理系统（装备）处理信息的保护需求。

### 密码产品安全防护需求分析

结合密码产品自身的运行环境、操作使用方式，分析密码产品面临的外部、内部安全风险，论证提出密码产品的密码资源保护、开机认证、前向安全、自检、密码资源销毁和物理防护等方面的安全防护需求。

### 密码资源管理保障需求分析（可选）

阐述密码产品可依托的密码基础设施（管理设备）部署情况，结合为密码资源管理保障所提供的信道、开放的端口等，分析产品密钥的管理保障需求。同时分析密码资源分发、管理信息传输过程所面临的风险和攻击，给出密钥、管理信息的保护需求。

## 密码配用（密码产品或模块请分别参考对应模板）

### 密码算法配用

给出配用密码算法的名称、算法体制和用途，以及使用算法的密钥长度、分组长度、输出长度等。

### 密码算法工作模式配置

论证提出分组、杂凑等密码算法的工作模式，并以表格形式,给出密码算法、用途、工作模式、密码算法参数和所配置密码产品之间的对应关系。示例如下：

密码算法配置情况列表如下：

表1 配用密码算法

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 算法名称 | 使用密钥 | 用途 | 工作模式 | 所配置算法参数 |
| XX密码算法 | XXX密钥 | 对XX数据进行加密保护 | XX模式 | [算法参数名称、新参数或已用参数，已配置于XX密码系统（装备）] |
| …… |  | …… | …… | …… |

### 工作模式(可选)

对本项目中密码算法的工作模式进行逐一描述，要求必须辅以图示，必须明确输入因素、变换过程（如反馈截取等）、输出处理方式、填充方式（并注明是算法接口负责填充还是调用算法接口前填充），以及IV的生成方式和更换周期等。

## 密钥配用

描述项目的密钥配用设计。包括密钥结构、密钥种类和用途、分割要求、密钥保障设计等。

### 密钥种类

结合用户安全要求和密码产品安全防护要求，论证提出密钥的种类、分割方式。分别说明各密钥的长度和用途，并明确密钥在各产品中的具体配置情况。

### 密钥结构

阐述密钥的层次结构设计，各密钥之间的保护关系。

### 密钥管理保障

采用文字描述和列表相结合的方式，分别对用户应用类密钥、管理保障类密钥的管理保障方式进行阐述，具体包括：各密钥的分割配置方式、产生与分发方式、存储与保护方式、更换方式、过期密钥的处理方式（如自然覆盖、删除等）及提示措施（如告警、停止工作等）、销毁方式等内容。结合密码产品的配置数量、应用范围、互通范围和使用寿命，给出密钥总量需求估计，并对密钥更换周期、分发和更换方式等设置的合理性和可行性进行分析。

对于现制密钥，若采用物理噪声源产生，应明确噪声源型号是否属于军用噪声源推荐型号；若采用软噪声产生，应说明采用软噪声的理由，并对相应的产生原理进行描述。

对于密码管理系统、KDC等设备，除要描述自身的密钥管理保障外，还要说明其管理保障对象的密钥在本地存储、启用等方面的机制和方式。对于密码管理系统使用的消耗型预制密钥体，要说明其存储的新旧预制密钥体之间的衔接机制（如余量继续使用，或新密钥体覆盖旧密钥体等）。

详细阐述密钥制作、分发、更换的工作流程，分别说明离线、在线方式，以及各环节中执行的操作，涉及的接口、相关设备和载体等。

## 密码协议

描述项目的密码协议设计。

参考军用密码协议描述规范说明，以能够确保无二义性、支持密码协议测评验证为基准。

1、协议概述

以条目形式分别给出协议的应用场景及用途、安全目标、协议参与方、协议要素描述及相关符号定义与说明，并给出协议中使用的报文和数据帧格式。

2、协议交互流程

按照协议交互流程的实际步骤，详细描述在协议的每一步中协议参与方使用了哪些协议要素（如算法、参数、算法工作模式、密钥、随机数、口令、身份信息、时戳、序列号等）、执行的具体操作和密码运算、以及收发的消息流基本数据格式等。需提供简明图形表示，能够揭示数据流动的形式、方向以及协议运行过程中的每一个时间节点各方内部状态的转化情况。

3、协议安全性分析

协议设计方应提供有关协议安全性的定性和定量分析过程和结论。包括协议要素要求和对协议的抗已知攻击能力分析。

# 安全保密措施设计

描述产品保密安全措施的设计。如开机自检、噪声检验、开机身份认证、密钥及参数自检、密码要素存储保护、密码销毁、安全报警、物理防护等安全保密措施的具体实现。

## 密码资源保护机制

分段阐述算法参数、密钥等密码资源的存储和使用区域、存储加密保护、紧急销毁等内容。存储加密保护措施必须注明所保护对象的具体内容，即具体到参数、密钥或其他需要保护的资源，还应说明采取的保护方式，若基于算法实现，则应给出采用的算法、参数和密钥。紧急销毁措施需要明确写明紧急销毁的销毁操作方式、具体的销毁方式（如覆写随机数等方式），以及销毁的内容，并明确密码产品是否还能提供密码服务等。

## 故障诊断和处置机制

分段阐述算法自检、参数自检、密钥自检、噪声源自检、功能自检等措施实现的原理和方式，以及发现故障后中止密码服务运行、报警、上报应用系统等处置方式。

## 逻辑安全防护机制

分段阐述密码产品采取的访问控制、安全审计、操作系统安全增强、软件防篡改、远程（本地进程）监控、数据完整性保护、防网络入侵等方面的逻辑安全防护措施，以及密码服务、密码产品操作配置、远程密码管理、本地密码管理、密码资源注入等接口设置。

## 物理安全防护机制

分段阐述密码产品为抵御物理攻击采取的安全防护措施，如芯片防探测和抗能量分析、开盖销毁、机械锁、电磁泄漏防护等。

## 前向安全防护机制

公普产品根据实际需要，进行前向安全设计，并说明采用的机制或方式。

# 电子元器件国产化应用

描述军用电子元器件国产化思路与原则，明确品种国产比例、数量国产比例以及国产数费比，简述选用进口电子元器件的必要性、安全性和可保障性。

# 通用性设计

描述项目研制过程中将采用的可靠性、维修性、保障性、安全性、测试性、环境适应性等设计要求。包括研制过程的可靠性控制措施、硬件可靠性控制措施、软件可靠性控制措施、维修性控制措施、保障性控制措施等。

## 可靠性设计

包括可靠性模型、可靠性分配、可靠性预计、硬件可靠性设计和软件可靠性设计等方面内容。

## 维修性设计

包括维修性设计要求、维修性设计措施等方面内容。

## 保障性设计

说明系统运行和维护时所需的技术保障、环境保障等要求以及相应的保障方案，包括保障内容、保障手段、保障资源等。

## 安全性设计

说明为保证系统安全、稳定使用，进行的相关设计方案，如操作权限设计、越权告警设计、容错设计等。

## 测试性设计

说明为保证软件可测试性，进行的相关设计方案。

## 环境适应性设计

说明为满足环境适应性指标要求，进行的相关设计方案，如结构设计、热设计等方面的措施。

# 质量控制与标准化管理

## 质量控制要求

描述项目研制过程中将采用的质量控制措施。包括成立质量管理机构，制定质量保证大纲，制定技术设计质量控制、联试试用质量控制、技术资料质量保证等方面的内容。

有外协工作的，要制定外协质量控制措施。

## 标准化管理要求

描述项目研制过程中的标准化控制措施。包括标准化工作要求、标准化工作内容与实施方案、标准化工作组织、标准化管理等方面的内容。

# 关键技术分析

提出本项目研制中要解决的关键技术，并分析实现的可行性。

# 任务分工

列出主要参与研制单位（人员）及各单位（人员）的负责的工作。

# 进度安排

按照项目的阶段划分，分别描述各阶段的起止时间、应完成的工作。