投 标 邀 请

项目概况

国家信息技术安全研究中心量子保密通信安全服务应用网络及平台系统采购（招标编号：GXTC-D-22630663） 招标项目的潜在投标人应在北京市海淀区四季青常青路和泓四季六号楼国信招标会议室获取招标文件，并于2022年 7月27 日 09点30分（北京时间）前递交投标文件。

## 一、项目基本情况

项目编号：GXTC-D-22630663

项目名称：国家信息技术安全研究中心量子保密通信安全服务应用网络及平台系统采购

预算金额：77.2万元

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 包号 | 设备名称 | 单位 | 数量 | 金额（万元） | 最高投标限价（万元） |
| 01 | 量子安全服务平台一体机 | 台 | 1 | 5 | 20.2 |
| 量子随机数发生器 | 台 | 1 | 4 |
| 安全U盾 | 个 | 5 | 0.2 |
| 量子安全服务移动引擎 | 套 | 1 | 5 |
| 量子随机数发生器软件  | 套 | 1 | 1 |
| 密钥系统交换密码机软件 | 套 | 1 | 3.3 |
| 充注终端软件 | 套 | 1 | 1.6 |
| 安全邮件软件 | 套 | 4 | 0.1 |
| 02 | 多协议侧信道采集与分析软件 | 套 | 1 | 30 | 57 |
| 多协议故障注入与攻击软件 | 套 | 1 | 27 |

是否接受进口产品：否

本项目是否接受联合体投标：否

本项目是否接受分包：否

**投标人必须对招标内每包所有内容进行投标，不允许只投标每包其中的一部分，否则作为无效标处理。**

国家信息技术安全研究中心量子保密通信安全服务应用网络及平台系统采购。

交货时间：详见附件

交货地点：用户指定地点

合同履行期限：详见附件。

本项目（*是/否*）接受联合体投标：否

## 二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：无

3.本项目的特定资格要求：无

## 三、获取招标文件

时间：2022年 7月6日至2022年 7月13日，每天上午9:00至12:00，下午13:00至17:00（北京时间，法定节假日除外 ）

地点：北京市海淀区四季青常青路和泓四季六号楼国信招标

方式：

**方式：1、请在“国信招标集团单位入库在线申请系统”（http://user.gxzb.com.cn/ztb/unit/login/register.jsp）注册并填报相关信息（上述网址仅限电脑端浏览器使用，手机等移动端无法使用）。**

**2、在上述“国信招标集团单位入库在线申请系统”注册成功后，于2022年 7 月6日至2022年7月13日（每日9:00-12:00，13:00-17:00，周六、周日及法定节假日除外），将材料发送至guoxindyn@163.com，材料如下：**

**（1） 法人代表证明书及法人代表授权及被授权人的有效身份证明（加盖公章）扫描件**

**（2）报名信息编辑文字，包括：项目编号、项目名称、包号、投标单位名称、投标单位地址、联系人、联系人手机号、邮箱。**

**（3）标书款付款截图。**

**（4）邮箱主题为：项目名称-投标单位名称。**

**标书款账户：**

 **开户名称：国信国采（北京）招标咨询有限责任公司**

 **开户银行：平安银行北京神华支行**

**银行账号：30206095000330**

**3、特别提醒：投标单位在“国信招标集团单位入库在线申请系统”第一次注册时填报的人员，默认为该单位的主账号管理员。此次来报名的人员如发现本单位已注册，则不需要再注册。**

**售价：人民币 500元/包，售后不退。只有购买了招标文件并登记备案的投标人才有资格参与投标。售卖标书联系人：丁女士 010-87235330。**

## 四、提交投标文件截止时间、开标时间和地点

截止时间（开标时间）：2022年 7 月27 日09时30分（北京时间）

地点：北京市海淀区四季青常青路和泓四季六号楼国信招标地下一层小会议室

## 五、公告发布媒介及公告期限

本次招标公告在中国政府采购网（www.ccgp.gov.cn）上发布。

自本公告发布日起5个工作日。

## 其他补充事宜

 1.采购项目执行政府采购政策

（1）对小微企业的产品给予价格扣除（监狱企业、残疾人福利性单位视同小微企业；残疾人福利性单位属于小型、微型企业的，不重复享受政策）。

（2）优先采购节能环保产品（注：所采购的货物在政府采购节能产品、环境标志产品实施品目清单范围内，且具有国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书）。

2.本项目投标截止期前被“信用中国”网站（www.creditchina.gov.cn）中列入失信被执行人和/或重大税收违法案件当事人名单的供应商、被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商（处罚决定规定的时间和地域范围内），无资格参加本项目的采购活动。

3.单位负责人为同一人或者存在控股、管理关系的不同单位，不得同时参加本项目的投标。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加本项目投标。

##  4.银行账户信息

**保证金、标书款、服务费户：**

 开户名称：国信国采（北京）招标咨询有限责任公司

 开户银行：平安银行北京神华支行

 银行账号： 30206095000330

**请投标人在汇款时务必注明所投标项目的招标编号及款项用途，否则，因款项用途不明导致投标无效等后果由投标人自行承担。**

## 八、对本次招标提出询问，请按以下方式联系。

　　　1.采购人信息

名 称：国家信息技术安全研究中心

地址：北京市海淀区

联系方式：赵先生，18911228996

2.采购代理机构信息

名 称：国信国采（北京）招标咨询有限责任公司

地　址：北京市海淀区四季青常青路和泓四季六号楼国信招标

联系方式：丁亚男、张肃 010-87235338 15210148475

传　 真：010-87235165

电子信箱：guoxindyn@163.com

3.项目联系方式

项目联系人：丁亚男、张肃

电　话：010-87235338 15210148475

附件

**一、系统简介**

量子保密通信安全服务应用网络及平台将量子密钥资源通过量子安全介质产品（硬件或软件形态）融合到各类安全应用中，并对其密钥进行动态管理，提供任意多点间密钥协商、接入认证、访问控制等功能服务。主要实现密钥(量子随机数)充注和会话密钥(量子密钥)分发两个功能。密钥充注功能：量子密钥充注终端将量子随机数写入Ukey，Ukey通过离线方式插入移动终端使用；会话密钥分发功能：量子安全服务器移动引擎调度密钥系统交换密码机，将待分发量子密钥与量子随机数进行一次一密异或加密，然后分发给量子密钥应用终端。

系统中，量子安全服务平台一体机，是量子安全服务移动引擎、密钥系统交换密码机功能集成的一体机产品；量子安全服务移动引擎，基于量子随机数或量子密钥分发网络与密钥系统交换密码机，为移动终端等设备提供密钥服务，实现量子密钥分发管理与控制、量子密钥分发流程状态控制和数据监测、量子密钥的安全应用管理，支撑用户实现安全通信等业务。密钥系统交换密码机，负责获取量子随机数或量子密钥分发网络的密钥，并进行密钥的存储管理，提供密钥终端充注，将获取量子密钥作为会话密钥提供给移动终端用于加密通信。量子随机数发生器的主要作用是生成量子随机数，随机性来源于激光自发辐射光子的相位涨落，具有良好的量子随机性。充注终端软件，是对安全终端或安全介质进行量子密钥充注的软件，可安装于特定充注机或普通PC终端上，并为安全介质提供发卡绑定和密钥充注功能。安全介质安全U盾实现安全认证机制和高速数据加解密等功能，提供数据签名、验签、身份认证安全保护。终端软件安全邮件运行在应用终端操作系统中，封装了安全介质的调用接口以及量子安全服务平台的交互接口，并通过API给应用层APP提供统一密钥应用服务，包括会话密钥获取，邮件数据加解密等功能。

多协议侧信道采集与分析软件，具备对多协议/接口开发板芯片和密码模块等进行能耗采集和电磁采集与分析的功能，增加了国密算法的分析方法，用于开展对量子安全芯片、密钥系统交换机、安全U盾等密码相关产品进行侧信道分析研究。多协议故障注入与攻击软件，具备对多协议/接口开发板芯片和密码模块等，进行电压和时钟故障注入与攻击功能，增加了电压和时钟组合故障攻击方法，用于开展对量子安全芯片、密钥系统交换机、安全U盾等密码产品进行电压和时钟故障分析研究。

经费概算77.2万元。

二、采购总体安排

对照系统建设方案软硬件设备清单，结合各功能模块研发技术需求，计划组织装备采购工作，对照情况如下表所示。

| 采购项目情况 |
| --- |
| 采购项 | 采购内容 | 单位 | 数量 | 经费概算（万元） | 备注 |
| 量子保密通信安全服务应用网络及平台 | 量子安全服务平台一体机 | 台 | 1 | 5 |  |
| 量子随机数发生器 | 台 | 1 | 4 |
| 安全U盾 | 个 | 5 | 0.2 |
| 量子安全服务移动引擎 | 套 | 1 | 5 |
| 量子随机数发生器软件  | 套 | 1 | 1 |
| 密钥系统交换密码机软件 | 套 | 1 | 3.3 |
| 充注终端软件 | 套 | 1 | 1.6 |
| 安全邮件软件 | 套 | 4 | 0.1 |
| 多协议侧信道采集与分析软件 | 套 | 1 | 30 |
| 多协议故障注入与攻击软件 | 套 | 1 | 27 |

三、采购项目基本情况

量子保密通信安全服务应用网络及平台

该系统主要将量子密钥资源通过量子安全介质产品（硬件或软件形态）融合到各类安全应用中，并对其密钥进行动态管理，提供任意多点间密钥协商、接入认证、访问控制等功能服务。主要实现密钥充注和会话密钥分发两个功能。密钥充注功能：量子密钥充注终端将量子随机数写入Ukey，Ukey通过离线方式插入移动终端使用；会话密钥分发功能：量子安全服务器移动引擎调度密钥系统交换密码机，将待分发量子密钥与量子随机数进行一次一密异或加密，然后分发给量子密钥应用终端，对优势产品开展采购建设。

1.采购方式。公开招标。

2.采购内容及经费概算

主要包括量子安全服务平台一体机、量子随机数发生器、安全U盾、量子安全服务移动引擎、量子随机数发生器软件、密钥系统交换密码机软件、充注终端软件、安全邮件软件、多协议侧信道采集与分析软件、多协议故障注入与攻击软件等10个模块，经费概算77.2万元。

四、实施计划

1.自采购方案批复之日起，15日内完成采购信息发布；

2.信息发布后，20个工作日确定承制单位；

3.合同签订后20日交付验收。

附件：量子保密通信安全服务应用网络及平台系统采购方案

附件

量子保密通信安全服务应用网络及平台

系统采购方案

**一、采购方式**

公开发布采购信息，公开招标方式采购。

**二、采购内容及概算**

量子保密通信安全服务应用网络及平台主要包括量子安全服务平台一体机、量子随机数发生器、安全U盾、量子安全服务移动引擎、量子随机数发生器软件、密钥系统交换密码机软件、充注终端软件、安全邮件软件、多协议侧信道采集与分析软件、多协议故障注入与攻击软件等10个模块，经费概算77.2万元。

量子保密通信安全服务应用网络及平台系统采购经费概算如下表。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 包号 | 设备名称 | 单位 | 数量 | 金额（万元） | 合计（万元） | 总计（万元） |
| 01 | 量子安全服务平台一体机 | 台 | 1 | 5 | 9.2 | 20.2 |
| 量子随机数发生器 | 台 | 1 | 4 |
| 安全U盾 | 个 | 5 | 0.2 |
| 量子安全服务移动引擎 | 套 | 1 | 5 | 11 |
| 量子随机数发生器软件  | 套 | 1 | 1 |
| 密钥系统交换密码机软件 | 套 | 1 | 3.3 |
| 充注终端软件 | 套 | 1 | 1.6 |
| 安全邮件软件 | 套 | 4 | 0.1 |
| 02 | 多协议侧信道采集与分析软件 | 套 | 1 | 30 | 57 | 57 |
| 多协议故障注入与攻击软件 | 套 | 1 | 27 |

**三、技术要求**

**（一）01包技术要求**

**1.量子安全服务平台一体机**

量子安全服务平台一体机是将量子安全服务移动引擎、密钥系统交换密码机功能合一的一体机产品；量子安全服务平台一体机包含业务注册、量子密钥获取、密钥安全存储、密码算法运算、接入认证、会话密钥分发，停机销号，配置管理等功能，为终端数量较少的应用场景提供一种便捷部署的使用方式。

**功能指标如下：**

1. 支持密钥全生命周期安全的密钥管理：发卡充注、激活、销卡等；
2. 支持终端接入认证；
3. 支持统一配置管理；
4. 支持多点间密钥协商；
5. 电源接口支持热插拔，1+1冗余备份；
6. 具备网口和USB接口；

**性能指标如下：**

1. 单点支持接入并提供服务的终端数量：1万以上；
2. 单点支持每秒并发的密钥业务处理：20/s以上；
3. 获取会话密钥的延时：500ms以下。

**2.量子随机数发生器**

量子随机数发生器的主要作用是生成量子随机数，随机性来源于激光自发辐射光子的相位涨落，具有良好的量子随机性，输出的随机数可通过国密、NIST等随机性测试。

**功能指标如下：**

1. 安全的随机数源，利用激光器（荧光）自发辐射的随机特性，通过干涉仪进行干涉并维持两臂相位差为2kπ+π/2，将随机相位量子化波动信息转换为随机数输出。
2. 系统状态稳定：实时监测、控制系统状态；通过主动维稳算法保持系统稳定性；极端情况下，系统状态不稳定时停止随机数输出。
3. 安全的后处理：利用安全的Toeplitz矩阵处理随机数源；经过后处理单元处理的数据作为最终输出的量子随机数供用户使用。

**性能指标如下：**

1. 以太网口≥600Mbps；
2. USB接口≥200Mbps；
3. 启动时间：30S；
4. 光波长：1550.12±0.5nm；
5. 电压：AC220V ，功耗：30W；
6. 工作环境温度：0-40 ℃；

**3.安全U盾**

具备完善的安全认证机制和高速的数据加解密等功能。支持USB标准协议传输，即插即用，支持热插拔。

功能指标如下：

1. 支持AES-128、AES-192、AES-256、DES、3DES等国际标准算法；
2. 支持SM1、SM2、SM3、SM4等国家密码局标准算法；

**4.量子安全服务移动引擎**

量子安全服务移动引擎是整个量子安全服务平台的核心控制管理软件，基于量子随机数或量子密钥分发网络与密钥系统交换密码机为移动终端等设备提供密钥服务，支撑用户实现安全通信等业务。

引擎采用微服务架构，部署于量子安全服务平台一体机，负责整系统的运行管理，包含：终端应用、交换密码机、充注模块等设备的管理员/用户注册、接入认证管理，安全介质的发卡密钥充注、激活、销卡等安全介质全周期管理以及相关充注密钥信息管理，移动终端间的会话密钥获取等业务管理，交换密码机存储密钥的调配与管理，以及全网统一配置管理和状态监控等。

**功能指标如下：**

1. 密码服务平台软件不存储密钥明文；
2. 支持一次一密的会话密钥传输，支持一业一密应用；
3. 支持从量子密钥分发网络获取会话密钥；
4. 与应用终端间采用REST接口，方便开发。

**5.量子随机数发生器软件**

量子随机数发生器软件是配套量子随机数发生器的软件，用于量子随机数发生器设备上位机操作。

**功能指标如下：**

1. 提供SDK库供用户调用。

**6.密钥系统交换密码机软件**

密钥系统交换密码机软件，是量子安全服务平台一体机中密钥系统交换密码机配套软件。负责获取量子随机数或量子密钥分发网络的密钥，并进行密钥的存储管理，提供密钥终端充注，将获取量子密钥作为会话密钥提供给移动终端用于加密通信。

**功能指标：**

1. 配套量子安全服务平台一体机中，实现密钥管理配置功能；
2. 支持密钥全生命周期安全的密钥管理；
3. 支持充注密钥生成和存储管理功能；
4. 支持会话密钥生成和存储管理功能；
5. 支持终端接入认证；

**7.充注终端软件**

充注终端软件，是对安全终端或介质进行量子密钥充注的软件，可安装于特定充注机或PC终端上，为安全介质提供绑定和密钥充注功能。

密钥充注时将从密钥系统交换密码机获取到的量子随机数，充注到终端设备的安全介质内，用于对申请的会话密钥进行加解密。

**功能指标如下：**

1. 提供良好的人机交互界面；
2. 支持与量子安全服务移动引擎的接入认证；
3. 支持对各类安全介质（如U盾、SIM卡）的绑定和密钥充注；
4. 支持接入密钥系统交换密码机，获取密钥充注权限，并建立和密钥系统交换密码机的安全通道；
5. 支持对终端安全介质的批量写卡能力。

**8.安全邮件软件**

安全邮件在邮件客户端基本功能的基础上，对邮件正文以及附件进行加解密，每封邮件使用不同的密钥，邮件在中转环节均为密文传输，邮件服务器无法查看邮件明文，本地实现收取的邮件密文存储，仅在查看邮件时解密，确保邮件传输和存储的安全。邮件加密密钥通过量子安全服务平台在线获取，实现一邮一密。

**功能指标如下：**

1. 支持邮件正文和附件的分离加密；
2. 支持一邮一密；
3. 支持邮件加密可选择，默认加密；
4. 支持发件人转发权限设置，默认禁止转发，禁止转发时原邮件为密文；
5. 收取邮件本地密文存储，查看时解密，退出客户端后清除缓存明文；
6. 支持在线更新升级。

**01包技术指标要求如下表：**

**（\*代表核心技术指标 ，#代表重要技术指标无标识项表示一般技术指标）**

| **序号** | **指标项** | **指标要求** | **响应情况** | **备注** |
| --- | --- | --- | --- | --- |
|  | **量子安全服务平台一体机** | **功能要求** | \*支持密钥全生命周期安全的密钥管理：发卡充注、激活、销卡等； |  |  |
| \*支持终端接入认证； |  |
| \*支持统一配置管理； |  |
| \*支持多点间密钥协商； |  |
| #电源接口支持热插拔，1+1冗余备份； |  |
| #具备网口和USB接口； |  |
| **性能要求** | #单点支持接入并提供服务的终端数量≥1万以上； |  |
| #单点支持每秒并发的密钥业务处理≥20/s以上； |  |
| #获取会话密钥的延时≤500ms。 |  |
|  | **量子随机数发生器** | **功能要求** | \*安全的随机数源，利用激光器（荧光）自发辐射的随机特性，通过干涉仪进行干涉并维持两臂相位差为2kπ+π/2，将随机相位量子化波动信息转换为随机数输出。 |  |
| \*系统状态稳定：实时监测、控制系统状态；通过主动维稳算法保持系统稳定性；极端情况下，系统状态不稳定时停止随机数输出。 |  |
| \*安全的后处理：利用安全的Toeplitz矩阵处理随机数源；经过后处理单元处理的数据作为最终输出的量子随机数供用户使用。 |  |
| **性能要求** | 以太网口≥600Mbps； |  |
| USB接口≥200Mbps； |  |
| 启动时间：30S； |  |
| #光波长：1550.12±0.5nm； |  |
| 电压：AC220V ，功耗：30W； |  |
| 工作环境温度：0-40 ℃； |  |
|  | **安全U盾** | \*支持AES-128、AES-192、AES-256、DES、3DES等国际标准算法； |  |
| \*支持SM1、SM2、SM3、SM4等国家密码局标准算法； |  |
|  | **量子安全服务移动引擎** | \*密码服务平台软件不存储密钥明文； |  |
| \*支持一次一密的会话密钥传输，支持一业一密应用； |  |
| \*支持从量子密钥分发网络获取会话密钥； |  |
| #与应用终端间采用REST接口，方便开发。 |  |
|  | **量子随机数发生器软件** | \*提供SDK库供用户调用。 |  |
|  | **密钥系统交换密码机软件** | \*配套量子安全服务平台一体机中，实现密钥管理配置功能； |  |
| \*支持密钥全生命周期安全的密钥管理； |  |
| \*支持充注密钥生成和存储管理功能； |  |
| \*支持会话密钥生成和存储管理功能； |  |
| \*支持终端接入认证； |  |
|  | **充注终端软件** | #提供良好的人机交互界面； |  |
| \*支持与量子安全服务移动引擎的接入认证； |  |
| \*支持对各类安全介质（如U盾、SIM卡）的绑定和密钥充注； |  |
| \*支持接入密钥系统交换密码机，获取密钥充注权限，并建立和密钥系统交换密码机的安全通道； |  |
| \*支持对终端安全介质的批量写卡能力。 |  |
|  | **安全邮件软件** | \*支持邮件正文和附件的分离加密； |  |
| \*支持一邮一密； |  |
| #支持邮件加密可选择，默认加密； |  |
| \*支持发件人转发权限设置，默认禁止转发，禁止转发时原邮件为密文； |  |
| \*收取邮件本地密文存储，查看时解密，退出客户端后清除缓存明文； |  |
| #支持在线更新升级。 |  |

**（二）02包技术要求**

**1.多协议侧信道采集与分析软件**

多协议侧信道采集与分析软件，实现对被测产品的能量迹进行自动化采集、预处理及密钥分析，同时支持对开发板形态芯片、物联网安全终端、密码模块等产品的侧信道安全测试与分析。

**功能指标如下：**

1. 可基于多协议接口（SPI、UART、CAN、I2C、14443、7816（非智能卡形态））实现对开发板芯片、物联网终端、密码模块等产品进行电磁侧信道、功耗侧信道、电流侧信道的智能触发功能。
2. 可实现对AES,DES, 3DES,RSA,RSA-CRT,ECC（解密和签名）,SM2（解密和签名）,SM4 等国际和国密算法进行侧信道分析。
3. 提供可实现多协议接口功能的多协议侧信道采集模块，实现多协议接口侧信道采集功能。
4. 支持采用C#或JAVA开发集成驱动已有电磁移动台，实现多协议电磁信号采集；如无法控制，需提供此软件配套的电磁移动台及电磁采集探头等配套模块，实现上述多协议接口电磁信号采集。
5. 可控制Micropross MP300 TCL2，实现对非接智能卡的侧信道采集。
6. 支持的分析方法至少包括：SPA（简单能量攻击）、CPA（相关性能量攻击）、DPA（差分能量攻击）、MIA（互信息分析）、TA（模板攻击）、高阶 SCA（高阶侧信道攻击）、TVLA（测试向量泄露评估）、NICV信息泄漏分析、机器学习分析（AES、SM4、SM2）。
7. 支持常用预处理模块，至少包括滤波模块类、压缩类、曲线自相关类、互相关类、模式匹配类、平均和方差分析，频谱处理、曲线拼接等8大子模块，用户可以直接调用。
8. 支持力科和PICO等示波器自动化采集。
9. 兼容inspector软件数据格式，可转化matlab数据格式。
10. 支持xyz移动台限位功能，支持使用热力图显示扫描结果，并判定最大泄露物理位置。
11. 支持智能硬件触发，在上述通信协议中检测到用户自定义字段产生硬件触发。
12. 支持显示实时采集时间、预计总采集时间、曲线对应明密文数据、当前曲线条数实时显示等。
13. 支持用户二次开发，提供sdk，集成用户预处理模块；支持攻击脚本开发，脚本实时编译。
14. 支持单次、多次及扫描攻击等不同攻击方式。
15. 支持项目管理功能，曲线保存、读取、调用及报告生成。
16. 支持多线程数据处理，中文操作界面，攻击参数设置及算法分析模块支持图形化界面。
17. 支持自动控制被测样品的复位和断电再上电功能。

18）支持可配置触发延时参数功能，范围：4ns-400ms。

19）支持可配置触发电平参数功能，范围：0V-5V。

**2.多协议故障注入与攻击软件**

多协议故障注入与攻击软件，实现对被测芯片和电子安全产品的电压和时钟毛刺精准故障注入攻击，具备密钥破解、固件验签绕过等分析功能。

**功能指标如下：**

1. 可基于多协议接口（SPI、UART、CAN、USB、I2C、7816（非智能卡形态））对开发板芯片、物联网终端和密码模块等产品进行时钟毛刺、电压毛刺故障注入。
2. 可实现对AES,DES,3DES,RSA,RSA-CRT,ECC（解密和签名）,SM2（解密和签名）,SM4 等国际和国密算法进行故障分析。
3. 提供配套的可实现多协议接口功能的时钟、电压故障注入模块，实现多协议接口的时钟、电压故障注入功能。
4. 支持时钟毛刺、电压毛刺多维组合故障注入攻击。
5. 支持实时显示攻击次数、攻击耗时、参数设置、采集控制、数据显示、曲线显示等信息。
6. 支持自动标记故障注入类型，包括正常，等长，过长，过短，超时等，支持基于故障类型的实时排序，实时统计，颜色标记功能，支持用户自定义故障编号。
7. 支持力科和PICO等示波器自动化采集。
8. 支持智能硬件触发，在上述通信协议中检测到用户自定义字段产生硬件触发。
9. 支持热力图分析，直观展示攻击参数对攻击效果的影响。
10. 支持一键复现攻击，可以直接导入筛选得到的有效攻击参数，进行故障注入攻击。
11. 支持一键泛化攻击，可以直接导入筛选得到的有效攻击参数，并对攻击参数进行随机扰动，进行故障注入攻击。
12. 支持一键重放攻击，可以直接导入曲线文件中的攻击参数变化策略，进行故障注入攻击。
13. 支持故障数据软件模拟生成功能。
14. 支持自定义工具箱和算法库功能，支持各类设备或算法的组合使用。
15. 支持设备连接、断开以及独立调试功能等。
16. 支持用户二次开发，提供sdk，集成用户预处理模块，支持攻击脚本开发，脚本实时编译。
17. 支持多线程数据处理、中文操作界面，攻击参数设置及算法分析模块支持图形化界面。
18. 支持时钟毛刺、电压毛刺信号同步示波器监控功能。
19. 支持外部触发模式，被测样品提供触发信号。
20. 支持内部触发模式，设备通过协议通信提供触发信号。
21. 支持密码算法正确性自动化验证，包括SM2验签，SM4，AES，DES等。
22. 支持采集数据转存功能，可实现导出为txt，excel等格式。
23. 支持可配置电压毛刺深度参数功能，范围：-6.0V - +6.0V可调。
24. 支持可配置电压毛刺宽度参数功能，可调范围：4ns-4ms，步进：4ns。
25. 支持可配置电压毛刺串数量功能，范围：1- 250个。
26. 支持可配置时钟输出功能，范围：1KHz - 50MHz。
27. 支持可配置时钟毛刺深度功能，可调范围：-6.0V-+6.0V。
28. 支持可配置时钟毛刺宽度功能，可调范围：4ns-4ms。
29. 支持可配置时钟毛刺串数量功能，范围： 1- 250个。
30. 支持对被测样品断电再恢复功能，设置范围：1ms-500ms。
31. 支持对被测样品复位再恢复功能，设置范围：1ms-500ms。

**02包技术指标要求如下表：**

 **（\*代表核心技术指标 ，#代表重要技术指标无标识项表示一般技术指标）**

| **序号** | **指标项** | **指标要求** | **响应情况** | **备注** |
| --- | --- | --- | --- | --- |
|  | **多协议侧信道采集与分析软件** | \*可基于多协议接口（SPI、UART、CAN、I2C、14443、7816（非智能卡形态））实现对开发板芯片、物联网终端、密码模块等产品进行电磁侧信道、功耗侧信道、电流侧信道的智能触发功能。 |  |  |
| \*可实现对AES,DES, 3DES,RSA,RSA-CRT,ECC（解密和签名）,SM2（解密和签名）,SM4 等国际和国密算法进行侧信道分析。 |
| \*提供可实现多协议接口功能的多协议侧信道采集模块，实现多协议接口侧信道采集功能。 |
| \*支持采用C#或JAVA开发集成驱动已有电磁移动台，实现多协议电磁信号采集；如无法控制，需提供此软件配套的电磁移动台及电磁采集探头等配套模块，实现上述多协议接口电磁信号采集。 |
| \*可控制Micropross MP300 TCL2，实现对非接智能卡的侧信道采集。 |
| \*支持的分析方法至少包括：SPA（简单能量攻击）、CPA（相关性能量攻击）、DPA（差分能量攻击）、MIA（互信息分析）、TA（模板攻击）、高阶 SCA（高阶侧信道攻击）、TVLA（测试向量泄露评估）、NICV信息泄漏分析、机器学习分析（AES、SM4、SM2）。 |
| \*支持常用预处理模块，至少包括滤波模块类、压缩类、曲线自相关类、互相关类、模式匹配类、平均和方差分析，频谱处理、、曲线拼接等8大子模块，用户可以直接调用。 |
| \*支持力科和PICO等示波器自动化采集。 |
| \*兼容inspector软件数据格式，可转化matlab数据格式。 |
| \*支持xyz移动台限位功能，支持使用热力图显示扫描结果，并判定最大泄露物理位置。 |
| \*支持智能硬件触发，在上述通信协议中检测到用户自定义字段产生硬件触发。 |
| \*支持显示实时采集时间、预计总采集时间、曲线对应明密文数据、当前曲线条数实时显示等。 |
| \* 支持用户二次开发，提供sdk，集成用户预处理模块；支持攻击脚本开发，脚本实时编译。 |
| \*支持单次、多次及扫描攻击等不同攻击方式。 |
| #支持项目管理功能，曲线保存、读取、调用及报告生成。 |
| \*支持多线程数据处理，中文操作界面，攻击参数设置及算法分析模块支持图形化界面。 |
| \*支持自动控制被测样品的复位和断电再上电功能。 |
| \*支持可配置触发延时参数功能，范围：4ns-400ms。 |
| \*支持可配置触发电平参数功能，范围：0V-5V。 |
|  | **多协议故障注入与攻击软件** | \*可基于多协议接口（SPI、UART、CAN、USB、I2C、7816（非智能卡形态））对开发板芯片、物联网终端和密码模块等产品进行时钟毛刺、电压毛刺故障注入。 |  |
| \*可实现对AES,DES,3DES,RSA,RSA-CRT,ECC（解密和签名）,SM2（解密和签名）,SM4 等国际和国密算法进行故障分析。 |
| \*提供配套的可实现多协议接口功能的时钟、电压故障注入模块，实现多协议接口的时钟、电压故障注入功能。 |
| \*支持时钟毛刺、电压毛刺多维组合故障注入攻击。 |
| \*支持实时显示攻击次数、攻击耗时、参数设置、采集控制、数据显示、曲线显示等信息。 |
| \*支持自动标记故障注入类型，包括正常，等长，过长，过短，超时等，支持基于故障类型的实时排序，实时统计，颜色标记功能，支持用户自定义故障编号。 |
| \*支持力科和PICO等示波器自动化采集。 |
| \*支持智能硬件触发，在上述通信协议中检测到用户自定义字段产生硬件触发。 |
| \*支持热力图分析，直观展示攻击参数对攻击效果的影响。 |
| \*支持一键复现攻击，可以直接导入筛选得到的有效攻击参数，进行故障注入攻击。 |
| \*支持一键泛化攻击，可以直接导入筛选得到的有效攻击参数，并对攻击参数进行随机扰动，进行故障注入攻击。 |
| \*支持一键重放攻击，可以直接导入曲线文件中的攻击参数变化策略，进行故障注入攻击。 |
| \*支持故障数据软件模拟生成功能。 |
| #支持自定义工具箱和算法库功能，支持各类设备或算法的组合使用。 |
| \*支持设备连接、断开以及独立调试功能等。 |
| \*支持用户二次开发，提供sdk，集成用户预处理模块，支持攻击脚本开发，脚本实时编译。 |
| \*支持多线程数据处理、中文操作界面，攻击参数设置及算法分析模块支持图形化界面。 |
| \*支持时钟毛刺、电压毛刺信号同步示波器监控功能。 |
| \*支持外部触发模式，被测样品提供触发信号。 |
| \*支持内部触发模式，设备通过协议通信提供触发信号。 |
| \*支持密码算法正确性自动化验证，包括SM2验签，SM4，AES，DES等。 |
| \*支持采集数据转存功能，可实现导出为txt，excel等格式。 |
| \*支持可配置电压毛刺深度参数功能，可调范围：-6.0V - +6.0V。 |
| \*支持可配置电压毛刺宽度参数功能，可调范围：4ns-4ms，步进：4ns。 |
| \*支持可配置电压毛刺串数量功能，范围：1- 250个。 |
| \*支持可配置时钟输出功能，范围：1KHz - 50MHz。 |
| \*支持可配置时钟毛刺深度功能，可调范围：-6.0V-+6.0V。 |
| \*支持可配置时钟毛刺宽度功能，可调范围：4ns-4ms。 |
| \*支持可配置时钟毛刺串数量功能，范围： 1- 250个。 |
| \*支持对被测样品断电再恢复功能，设置范围：1ms-500ms。 |
| \*支持对被测样品复位再恢复功能，设置范围：1ms-500ms。 |

（三）质量控制

应答人必须向采购人提供满足本技术规格书所列举全部或大部分内容的实际可运行软件系统及必需的专用硬件，提供软件正常运行所需的通用硬件设备、网络环境和用电等方面的数量和参数配置要求，并在采购人指定的地点完成系统安装、联调、测试等工作，在系统实施过程中负责解决全部技术问题。若本技术规格书中的软件系统和专用硬件在配置或要求方面出现不合理或不完整的问题，应答人有责任和义务提出补充修改方案并征得采购人同意后付与实施。

为保证系统的质量和系统研制的顺利推进，采购人的技术人员可以全程参加项目的实施工作，包括总体规划、方案设计、系统实现、系统内部测试、系统试运行以及系统检验、系统测试、产品验收等过程。应答人必须给予全面的支持和配合。

1.质量管理

应答人应建立严格的质量保证体系，制定项目开发建设质量控制方案和实施措施，并督促落实各环节质量控制内容和目标；保证总体规划、方案设计、系统实现、系统内部测试与试运行各个阶段工作满足采购人对质量的要求。

应答人应根据整个项目开发的工作计划，对阶段性工作成果进行审查和测试，并向采购人提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个系统开发实施的质量。

应答人有责任且必须承诺使采购人在本技术规格书中说明的全部或大部分功能指标能够实现，并实现系统的有效集成，且系统的投入运行不能影响采购人现有其他系统的正常安全运行。

质量管理由应答人自行组织，并向采购人提交相应的质量管理报告。采购人可以随时检查应答人的质量管理方式、措施和流程。

在系统交付之前，应答人有责任根据采购人的要求，对部分涉及到与其他子系统有功能和/或数据交互的模块进行适当的调整或修改。

2.系统检验

检验项目包括本技术规格书规定的，且是应答人可以实现的项目。

除合同或订单中另有规定外，应答人负责完成本规格书规定的检验项目。必要时，采购人或上级鉴定机构有权对规范所述的任一检验项目进行检查。

鉴定检验顺序为：系统组成检验、功能检验、性能检验、使用要求检验（含维修性检验）。

检验方法分为目测检验、安装检验和使用测试检验；检验数据为系统在用户操作下获得的数据。

系统检验由应答人自行组织，并向采购人提交相应的系统检验报告。

3.系统测试

应答人应提前按照采购人提出的系统使用要求和通用指标要求，或专门提供的系统运行环境要求拟制系统部署方案，包括所需要的硬件设备型号和数量、支撑软件系统、网络构成及配置和带宽、电源、布线及各种跳线设置等要求，协助采购人实施部署，并与采购人或采购人指定的系统集成与运维服务厂商进行调试、测试与最终验收。

应答人应在系统交付时提供采购人认可的测试大纲、测试细则并配合采购人进行系统测试。

应答方应按照技术规格书的要求，协助采购人或采购人指定的系统集成与运维服务厂商对系统的功能、性能进行测试，对使用要求和通用指标符合度进行测试或检查，并形成测试报告。

系统测试完成并经采购人认可后才能投入运行和组织产品验收。

系统测试由采购人或采购人指定的系统集成与运维服务厂商组织，应答人参与并配合。

4.系统验收

在技术规格书规定的环境和条件下, 系统能够正常运行, 并达到技术规格书明确的功能和性能指标要求。

 系统在测试过程中出现的系统功能、性能指标，或者使用要求和通用指标符合度不满足技术规格书和合同时，采购人有拒收的权利。

 测试完成后，采购人可以根据测试情况和测试报告，按照相关规定和程序组织对系统的验收。

 系统验收由采购人组织，应答人配合。

（五）通用要求

1.环境适应性要求

系统以软硬件形式部署在机房和实验室，工作温度为室温。

2.保障性

系统应配备方便维护和检测所需的附件、工具及技术资料。

四、商务要求

（一）交付要求

应答人应提供与整个系统研制有关的技术文档，包括总体规划、方案设计、系统实现、系统内部测试、系统试运行、维护管理体系对应的全部技术文档和管理规范。技术文档应该全面、完整、详细、清晰，且与系统相一致，能够满足采购人对系统的安装、使用、维护、二次开发的需要。技术文档一般为中文。

 技术文档应当包括与运行版本一致的总体设计方案(含系统软硬件组成)、软件需求规格说明、软件设计说明、内部测试报告、软件用户手册、软件研制工作总结、可执行代码、源代码(以合同或订单规定为准)以及其它配套资料。

 技术文档内容应满足《计算机软件产品开发文件编制指南》和《软件工程术语》的要求。提供的技术文档均应以纸张或光盘为载体，除可执行代码和源代码外，文档的格式可为.DOC、.DOCX、.PPT、.PPTX、.XLS、.XLSX、.RTF或.PDF中任意一种类型的文件。

 系统交付由采购人或采购人指定的系统集成与运维服务厂商组织，应答人参与并回答和解决与交付有关的问题。

系统交付时，采购人应按采购方案中的技术要求及指标要求编写测试方案，组织产品验收测试，通过测试有方可接收。

（二）付款方式

产品经验收合格后，采购方按合同约定方式进行支付。

（三）安装调试

由中标单位应按照采购方要求，按照采购方指定的时间、地点对设备进行安装调试，期间产生的线材及服务不再收取任何费用。

（四）服务及培训

应答人提供现场技术培训，时间、培训地点应和采购人协商。

（五）保证和售后服务要求

★（1）质量保证期：合同项中产品的质量保证期为产品安装验收合格之日起整机硬件/软件全保不低于三年。

（2）保证期内免费软件升级服务。在保证期限内，乙方应配合采购方对产品进行维护检查，在正常使用条件下，若产品出现故障，厂商要在用户报修后2小时内响应，48小时内到场修复。在响应时间内不能修复时，厂商须免费提供备机、备件，保障用户业务不间断。厂商提供上门维修服务，免除包括人力和零部件一切费用。

（3）在质量保证期限以外，产品使用中出现质量问题，乙方应根据甲方要求提供现场技术服务，以成本价收取人工和部件费用。

（4）维修中需更换的零部件要保持其原有技术特性，硬盘免回收。