

附件 2

2023 年度第三期国产 IP 核资源

序号	IP 名称	IP 说明	IP 供应商	可支持项目数
1	RISC-V 处理器 IP 核	对标 Cortex-M3（具体参数详见具体参数详见国产 IP 参数）	芯来智融半导体科技(上海)有限公司	0
		对标 Cortex-M4/M4F（具体参数详见国产 IP 参数）		1
2	多次可编程存储器 IP 核	适用于逻辑工艺;高可靠性;最多额外增加 1 层的光罩;超过 1 万次的程序擦写;高速率&低功耗（具体参数详见具体参数详见国产 IP 参数）	成都锐成芯微科技股份有限公司	3
3	密码 IP 核	符合国家密码局要求的国产密码算法模块和真随机数发生器模块（具体参数详见具体参数详见国产 IP 参数）	深圳市纽创信安科技开发有限公司	1

以上国产 IP 核具体参数如下：

一、系列 RISC-V 处理器 IP 核

RISC-V 处理器 IP 能满足 AIoT 时代的各类需求，广泛应用于物联网、工业控制、存算一体、AI 以及汽车电子等，其架构具体开放性、先进性、简洁性、模块化、扩展性五大特点，本次采购的 RISC-V 处理器 IP 具体要求为：

（一）支持 RV32I/EMACB 指令集、2 级流水线、可配置本地存储单元、硬件乘除法器、I-Cache、可信执行环境 TEE 等。 1.64/3.66 DMIPS/MHz (Legal/Best Effort), 3.78 CoreMark/MHz（对标 ARM Cortex-M0/M0+、M3、M23）。

（二）支持 RV32IMACFDPB 指令集、3 级流水线、可配置 SIMD DSP 扩展、单/双精度浮动、硬件乘除法器、I-Cache/D-Cache、可信执行环境 TEE 等。 1.89/3.68

DMIPS/MHz (Legal/Best Effort)、4.02 CoreMark/MHz (对标 ARM Cortex-M33、M4、M4F)。

(三) 支持 RV32IMACFDPB 或 RV64IMACFDPB 指令集、6 级流水线、可配置 SIMC DSP 扩展、单/双精度浮动、L2 Cache、MMU、硬件乘除法器、I-Cache/D-Cache、可信执行环境 TEE 等。 1.65/4.2 DMIPS/MHz (Legal/Best Effort), 3.5 CoreMark/MHz (对标 ARM Cortex-M7、R4、R5、A5、A7)。

二、多次可编程存储器 IP 核

多次可编程存储器 (Multi Time Programmable 存储器) IP 可多次编程, 具有实现灵活配置的数据存储能力, 可以复用到各种 IC 设计中。适用于既要有一定配置灵活性, 又要有低成本需求, 主要应用于需要迅速量产的便携式 IC 产品。本次采购的多次可编程存储器 IP 核具体要求为:

(一) 嵌入式应用要求: MTP 存储器 IP 能够满足多种嵌入式应用领域包括: MCU 的存储单元、取代传统 OTP、eFlash、CMOS 图像传感器修复、数据存储、射频识别技术中标识信息的存储以及 SoC 中初始信息的存储等等。

(二) 容量要求: MTP 存储器 IP 的容量要求在 32bit 至 1Mbit 之间, 数据宽度在 8bit 到 64bit 之间, 能够根据客户的需求灵活配置。

(三) 技术要求: 存储单元采用 2T1C 结构, 根据应用支持高密度 HD (High Density)、高可靠性 HR (High Reliability)、超低功耗 ULP (Ultra Low-Power) 等三种技术模式, 技术细节详见下表:

工艺模式	高密度 HD	高可靠性 HR	超低功耗 ULP
标准制程	√	√	√
额外的光罩层	1-2	0	1
逻辑工艺的兼容性	√	√	√
晶圆生产成本	标准的逻辑工艺相当	标准的逻辑工艺相当	标准的逻辑工艺相当
工艺相关性	低	低	低
制程开发时间	6 个月	6 个月	6 个月
技术可测性	高	高	高
系统内可编程	√	√	√
可擦除	√	√	√
存储单元大小	小	中	中
快速对接代工厂/工艺	√	√	√
数据保持时间	10 年	10 年	10 年
消费级产品	√	√	√
工业级产品	√	√	√
汽车级产品		√	

（四）工艺要求：MTP 存储器 IP 采用标准的 CMOS 逻辑工艺实现；要能支持主流代工厂商的主流标准生产工艺。具体包括：

代工 厂 工艺	中芯 国际	格罗 方德	台联 电	华虹 宏力	合肥 晶合	华润 上华	粤芯	积塔	中芯 绍兴	矽佳
0.18um	√	√	√	√		√	√	√	√	√
0.15um						√				√
0.13um	√									√

0.11um	√		√		√					√
90nm	√			√						

注：√代表 IP 必须支持该工艺

三、密码 IP 核

密码是保障网络空间安全的核心技术支撑。密码技术已经在金融、国家电网、交通、教育等很多领域得到广泛应用。通信网络、物联网、大数据、云计算、人工智能、工业互联网、网络安全等信息技术对保障网络安全提出了新挑战。本次采购的采购标的为符合国家密码局要求的国产密码算法模块和真随机数发生器模块，包括加解密的 SM2 算法硬件模块、SM3 算法硬件模块、SM4 算法硬件模块和真随机数发生器硬件模块。技术要求为：

标的产品	指标项	指标要求
SM2（国密标准非对称密码算法模块）	1 SM2（国密标准非对称密码算法模块）	
	1-1 硬件 IP 性能	签名 ≥ 30 次/s；验签 ≥ 15 次/s @100MHz
	1-2 IP 接口	AXI 或 AHB
	1-3 IP 工作温度范围	-25℃至 85℃
	*1-4 硬件 IP 安全性	符合国密一级要求
	1-5 可靠性	可以正常运行 10 年以上
	1-6 代码要求	支持 FPGA 集成和 ASIC 集成
SM3（国密标准散列函数模块）	2 SM3（国密标准散列函数模块）	
	2-1 硬件 IP 性能	50Mbps @100MHz
	2-2 IP 接口	AXI 或 AHB
	2-3 IP 工作温度范围	-25℃至 85℃
	*2-4 硬件 IP 安全性	符合国密一级要求
	2-5 可靠性	可以正常运行 10 年以上
	2-6 代码要求	支持 FPGA 集成和 ASIC 集成
	2-7 使用案例	提供 2 个以上使用案例文档（合同或应用报告）
SM4（国密标准对称密码算法模块）	3 SM4（国密标准对称密码算法模块）	
	3-1 硬件 IP 性能	100Mbps @100MHz
	3-2 IP 接口	AXI 或 AHB
	3-3 IP 工作温度范围	-25℃至 85℃
	*3-4 硬件 IP 安全性	符合国密一级要求

	3-5 可靠性	可以正常运行 10 年以上
	3-6 代码要求	支持 FPGA 集成和 ASIC 集成
TRNG（真随机数发生器模块）	4 TRNG（真随机数发生器模块）	
	4-1 硬件 IP 性能	大于 1.5Mbps
	4-2 IP 接口	AXI 或 AHB
	4-3 IP 工作温度范围	-25℃至 85℃
	*4-4 硬件 IP 安全性	符合 GM 0008-2012
	4-5 可靠性	可以正常运行 10 年以上
	4-6 工艺依赖	不依赖工艺
	4-7 代码要求	支持 FPGA 集成和 ASIC 集成
	4-8 测试报告	提供第三方符合 GM 0008-2012 硅测试报告