



MSL FPGA INC 晶片參數

■ 芯片概述

DS28C40G/V+U是来自MSL FPGA INC美时龙的DeepCover安全认证芯片，专为高安全需求场景设计。

以下是其核心信息：

■ 核心参数

接口：I2C兼容（SCL/SDA引脚），支持标准模式（100kHz）和快速模式（400kHz）

加密引擎：集成ECC-P256（非对称）和SHA-256（对称）硬件加速器，支持FIPS 180-4标准。

存储器：6KB OTP（一次性可编程）存储器，用于存储密钥、证书及用户数据。

安全特性：内置真随机数发生器（TRNG）、64位唯一ROM ID、防篡改检测机制。

■ 功能特性

双向认证：支持基于ECC-P256的ECDSA签名验证及SHA-256 HMAC认证，确保设备身份合法性。

安全引导：通过GPIO引脚实现主机处理器安全启动验证，防止未授权固件加载。

灵活配置：GPIO可编程为安全/非安全模式，支持密码可靠操作。

防攻击设计：采用DeepCover技术，集成芯片屏蔽、密钥加密及主动反制措施。

■ 应用场景

汽车电子：ECU模块安全认证、固件防篡改保护。

工业物联网：设备身份验证、IP保护及授权管理。

医疗设备：确保数据完整性与操作合规性。

消费电子：高端外设（如打印机耗材）防伪认证。