

N32S035

产品简介

N32S035采用 32 bit ARM Cortex-M0内核，最高工作主频80MHz，用户可用空间100KB FLASH，集成UART和I2C通信接口，以及用于加密算法的内置硬件加速引擎

关键特性

- 内核 CPU
 - 32 位 ARM Cortex-M0 内核，单周期硬件乘法指令
 - 最高主频 80MHz
- 安全存储器
 - 用户可用空间 100KByte 片内 FLASH，支持加密存储，支持硬件 ECC 校验，10 万次擦写次数，10 年数据保持
- 低功耗管理
 - RUN 模式：12mA@VCC=3.3V/25℃，系统时钟 80MHz
 - STOP 模式：75uA@VCC=3.3V/25℃，唤醒后继续执行程序
 - STANDBY 模式：2uA@VCC=3.3V/25℃，唤醒后从 0 地址运行，SRAM 数据不保持
- 时钟
 - 内部高速时钟 80MHz
- 复位
 - 支持上电/掉电复位
 - 支持外部复位源复位
 - 支持芯片异常复位
 - 支持低功耗模式复位
- 通信接口
 - 1 路 UART 接口，最高速率达 256000 bps
 - 1 路复用 I2C 接口，最高速率达 3.4Mbps，仅支持从模式
- 最大支持 5 个支持复用功能的 GPIO
- 编程方式
 - 支持 UART Bootloader 和 I2C Bootloader
- 安全算法
 - 支持标准 FIPS 186 中规定的 ECDSA（支持 NIST 曲线 p256/p384/p521）、RSA2048/3072/4096 数字签名算法（v1.5 与 PSS）
 - 支持 SP 800-56 中规定的 ECDH(E)算法（支持 NIST 曲线 p256/p384/p521）
 - 支持 PKCS#1 中规定的 RSA2048/3072/4096 加解密算法（v1.5 与 OAEP）
 - 支持 FIPS 180 中规定的 SHA-1、SHA-256、SHA-384、SHA-512 哈希函数

- 支持 FIPS 197 中规定的 AES (128/256) 分组密码算法, 支持 CBC, ECB, CTR, OFB, CCM, GCM 模式
- 支持 GM/T 0003 中规定的 SM2 数字签名、加密解密及密钥协商
- 支持 GM/T 0004 中规定的 SM3 杂凑密码算法
- 支持 GM/T 0002 中规定的 SM4 分组密码算法, 支持 CBC, ECB, CTR, OFB, GCM 模式
- 支持 SP 800-90 (A/B/C) 的随机数发生器
- 支持 SP 800-108 中规定的密钥派生函数
- 支持 SP 800-224 中规定的 HMAC
- 随机数质量符合 GM/T 0005 和 SP 800-22 的要求
- 支持 TLS v1.2 PRF 和 HKDF

● 安全 API

- 设备管理, 支持设备信息获取等接口
- 应用管理, 访问控制的客体, 包含多个容器和文件。支持应用的创建、枚举、删除、打开、关闭等操作
- 容器管理, 密钥存储的数据结构, 含容器的创建、删除、枚举、打开和关闭操作, 也支持获取容器类型、导入数字证书和导出数字证书操作
- 文件管理, 用于支持用户扩展开发, 包括创建文件、删除文件、枚举文件、获取文件信息、文件读操作、文件写操作等
- 访问控制, 设备认证、PIN 码管理和安全状态管理操作。可用于修改管理员 PIN 和用户 PIN 的值, 获取 PIN 码信息 (如最大重试次数、当前剩余重试次数等), 校验 PIN 码等功能
- 密码服务, 提供对称算法运算、非对称算法运算、密码杂凑运算、密钥管理和消息鉴别码计算功能, 密钥生成、密钥导入、密钥导出、密钥销毁等功能。
- 安全信道建立, 支持与主机端建立安全通道

● 安全校验

- CRC16 运算

● 安全防护

- 支持电压异常检测、温度异常检测、激光注入检测
- 时钟加扰
- 总线加密
- 存储器加密、分区保护
- 计时攻击、能量攻击、电磁攻击等侧信道技术防护
- 故障注入防护
- Glue Logic、Active Layer (MESH)、Passive Layer

● 128 位 UID

● 工作条件

- 工作电压范围: $1.8 \pm 5\%V$, $3.3 \pm 10\%V$

- 工作温度范围: $-40 \sim 105^{\circ}\text{C}$
- ESD: $\pm 4\text{KV}$ (HBM 模型) / $\pm 500\text{V}$ (CDM 模型)
- 封装
 - DFN8
- 安全认证
 - EAL5+
 - FIPS 140-3 CMVP Level 3
- 中间件
 - OpenSSL

目 录

关键特性	1
1.1 产品资源配置	5
2 封装	5
2.1 DFN8封装	5
2.1.1 DFN8引脚分布	5
2.1.2 DFN8封装尺寸	6
3 版本历史	7
4 声明	8

1.1 产品资源配置

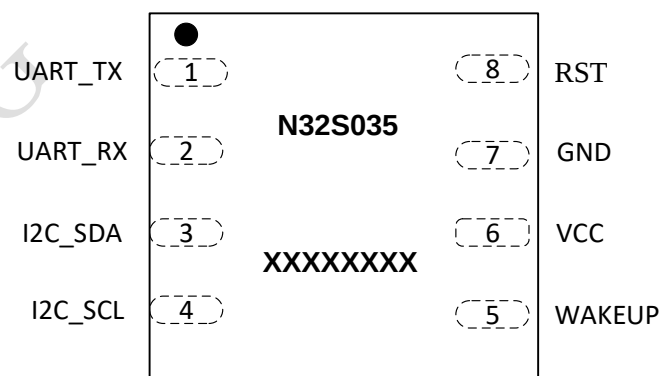
器件型号		N32S035
用户可用 FLASH 容量 (KB)		100
CPU 频率		ARM Cortex-M0 @80MHz
工作环境		1.8±5%V, 3.3±10%V / -40 ~ 105℃
通讯接口	I2C	1
	UART	1
GPIO		5
算法支持		RSA2048（签名验签/加密解密）、ECDSA（NIST p256/p384/p521）、ECDH（NIST p256/p384/p521）、SM2（数字签名/加密解密及密钥协商）、AES（128/192/256）及 CBC/ECB/CTR/OFB/GCM 模式、SM4 及 CBC/ECB/CTR/OFB/GCM 模式、SM3、SHA-1/SHA-224/SHA-256/SHA-384/SHA-512、随机数发生器
安全保护		时钟加扰、总线加扰、存储器加密、分区保护、电压/温度异常检测、激光注入检测、计时/能量/电磁侧信道攻击防护、故障注入防护、Glue Logic、Active Layer (MESH)、Passive Layer
安全 API		设备管理、应用管理、容器管理、文件管理、访问控制、密码服务，支持 TLS v1.2 PRF 和 HKDF
封装		DFN8

2 封装

芯片的UART_TX、UART_RX、I2C_SDA、I2C_SCL和WAKEUP管脚支持复用成普通GPIO。

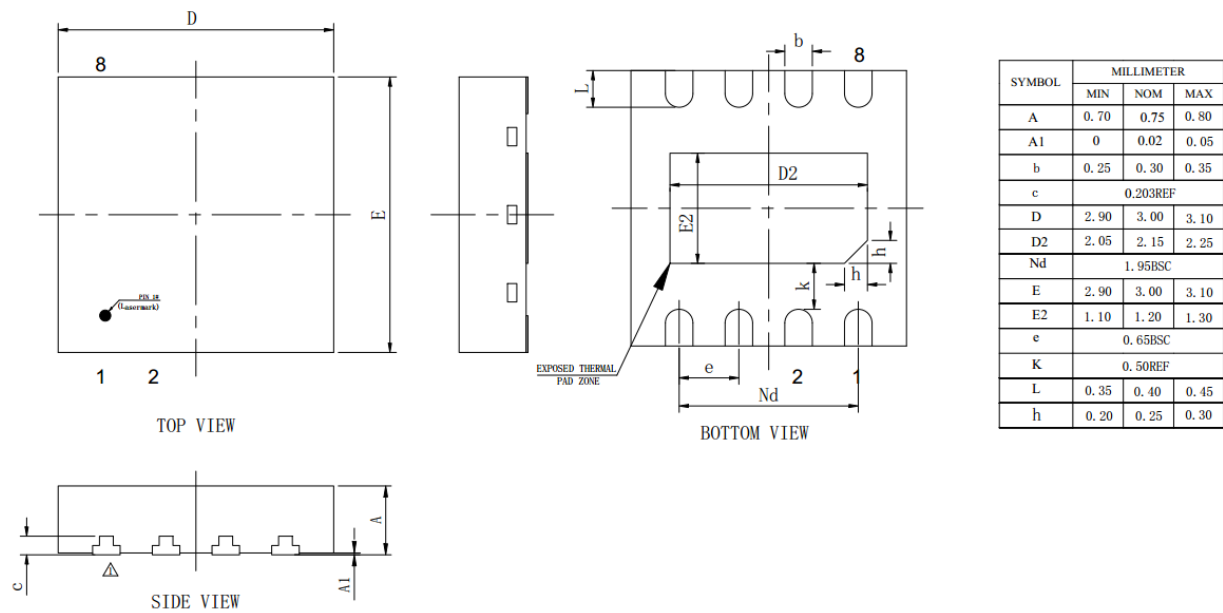
2.1 DFN8封装

2.1.1 DFN8引脚分布



注：“N32S035”为芯片产品名称，“XXXXXXXX”为生产批次号。

2. 1. 2DFN8封装尺寸



3 版本历史

日期	版本	修改
V1.0.1	2025.01.09	初始版本

NSING CONFIDENTIAL

4 声明

国民技术股份有限公司（下称“国民技术”）对此文档拥有专属产权。依据中华人民共和国的法律、条约以及世界其他法域相适用的管辖，此文档及其中描述的国民技术产品（下称“产品”）为公司所有。

国民技术在此并未授予专利权、著作权、商标权或其他任何知识产权许可。所提到或引用的第三方名称或品牌（如有）仅用作区别之目的。

国民技术保留随时变更、订正、增强、修改和改良此文档的权利，恕不另行通知。请使用者在下单购买前联系国民技术获取此文档的最新版本。

国民技术竭力提供准确可信的资讯，但即便如此，并不推定国民技术对此文档准确性和可靠性承担责任。

使用此文档信息以及生成产品时，使用者应当进行合理的设计、编程并测试其功能性和安全性，国民技术不对任何因使用此文档或本产品而产生的任何直接、间接、意外、特殊、惩罚性或衍生性损害结果承担责任。

国民技术对于产品在系统或设备中的应用效果没有任何故意或保证，如有任何应用在其发生操作不当或故障情况下，有可能致使人员伤亡、人身伤害或严重财产损失，则此类应用被视为“不安全使用”。

不安全使用包括但不限于：外科手术设备、原子能控制仪器、飞机或宇宙飞船仪器、所有类型的安全装置以及其他旨在支持或维持生命的应用。

所有不安全使用的风险应由使用人承担，同时使用人应使国民技术免于因为这类不安全使用而导致被诉、支付费用、发生损害或承担责任时的赔偿。

对于此文档和产品的任何明示、默示之保证，包括但不限于适销性、特定用途适用性和不侵权的保证，国民技术可在法律允许范围内进行免责。

未经明确许可，任何人不得以任何理由对此文档的全部或部分进行使用、复制、修改、抄录和传播。