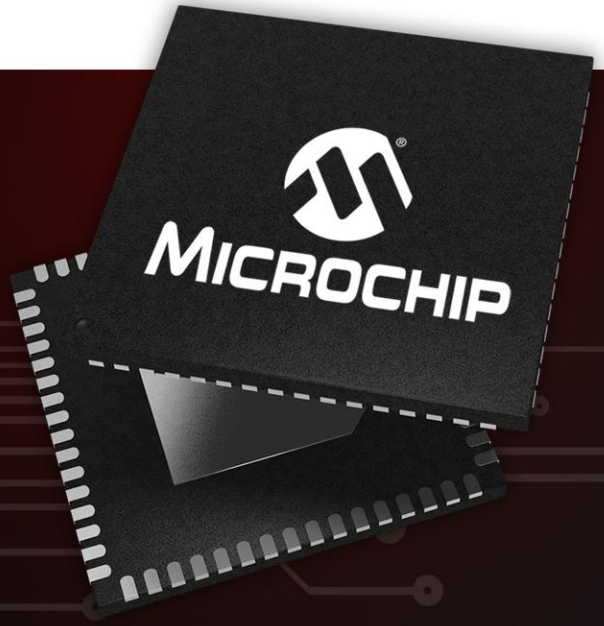
MICROCHIP



A Leading Provider of Smart, Connected and Secure Embedded Control Solutions




王军，资深应用工程师

2019年12月12日

Microchip嵌入式安全方案在IoT产品中的应用

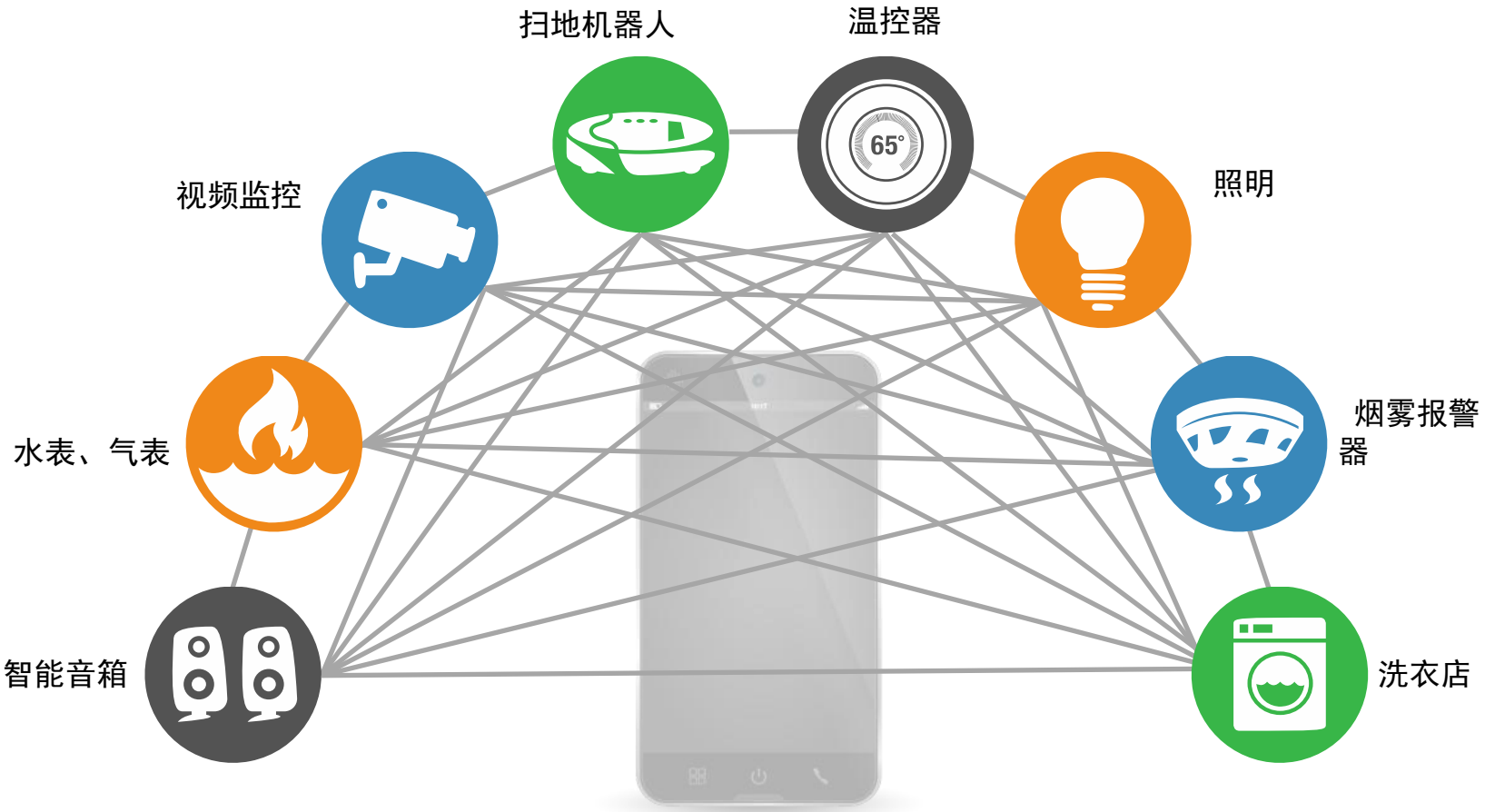
议 程

- IoT行业面临的安全挑战
- 介绍Microchip的安全产品
- 使用Microchip的整体方案快速接入云架构
- 总结：Microchip安全方案的优势

© 2019 Microchip Technology Inc. All Rights Reserved.

IoT行业面临的安全挑战

万物互联的IoT



国际数据公司(IDC)的数据显示，2018年全球物联网支出预计将达到**7725亿**美元。这比2017年用于物联网的6740亿美元增加了**15%**。(1)

(1) https://softwarestrategiesblog.com/2018/01/01/roundup-of-internet-of-things-forecasts-and-market-estimates-2018/

© 2019 Microchip Technology Inc. All Rights Reserved.

在安全中密钥的重要性

- **安全：关键是密钥**

- 一个密码系统应该是安全的，如果系统的一切——除了密钥——都是公开的。 **-- Kerckhoff's Principle**

真实的私钥看起来像这样的：
JVFDvdfvJvfdnjvjk543524cds9ics9cCDSCcs0dcw8eidpciswsn8934XSCDS

- 敌人知道这个系统

  Claude Shannon

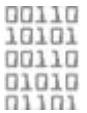
- **为什么密钥很重要？拥有密钥后，可以冒充身份执行核心事务**

© 2019 Microchip Technology Inc. All Rights Reserved.

如今存在的薄弱环节

安全性是设计出来的：目前嵌入式安全性已经在设计上被考量，但是难以实现

教育缺失：信任链没有被很好地理解，再加上原理复杂，难以执行，因此没有合理的实施



密钥/证书处理不当：私钥直接放在软件中，并且很容易被读出来

后门对黑客开放：他们攻击物联网中最薄弱的环节，即不安全的软件，并利用用户的习惯

制造过程不可靠，不安全：造成安全泄漏或过度构建等问题

© 2019 Microchip Technology Inc. All Rights Reserved.

嵌入式安全典型的应用场景

所有这些功能都需要相关的密码算法，而核心就是密钥的安全

应用层安全	利用系统的加密功能进一步加强实现(访问权限—特权)
安全连接	验证和加密设备通信
安全升级	利用安全的通信和安全的启动机制，以确保安全交付真实的映像
IP 保护	防止对手窃取驻留在MCU固件或FPGA RTL中的IP
防假冒和防克隆	防止对手假冒一次性用品(墨盒)或者克隆配件
硬件的信任根	可信赖的身份 固件验证(也称为安全启动—适用于所有系统)

单片机
32/16/8位
如：Arm® Cortex®-M23+

微处理器
Arm® Cortex®-A5

安全器件
Common Criteria (JIL) 评分高

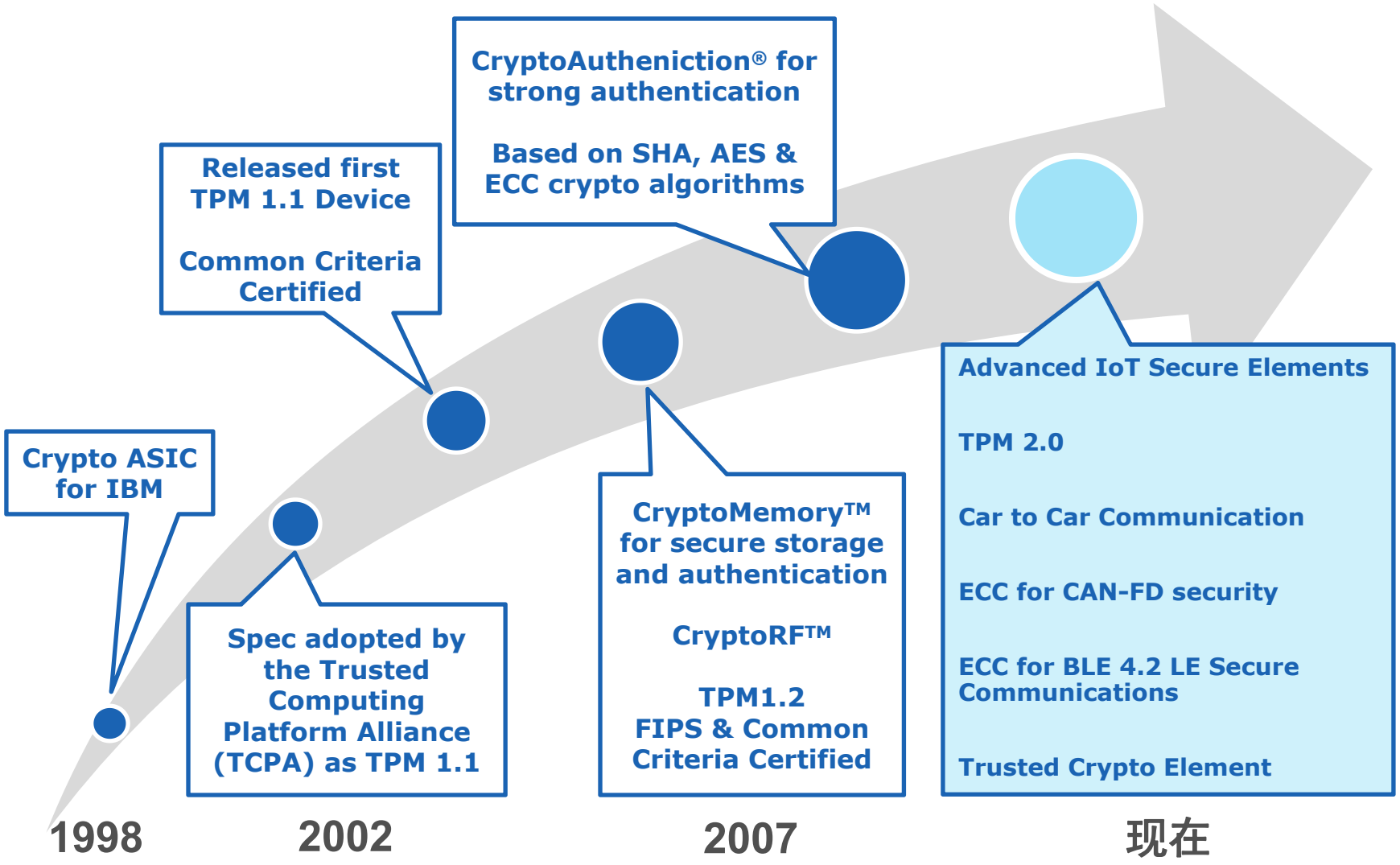
网络控制器
有线和无线
集成通信协议栈

FPGA
解决方案

© 2019 Microchip Technology Inc. All Rights Reserved.

Microchip的安全产品

Microchip安全产品的历史



© 2019 Microchip Technology Inc. All Rights Reserved.

Microchip SE 安全组件产品线

明星产品

	AES132	ATSHA204A	ATECC508A	ATECC608A	TPM 1.2	TPM 2.0
主要特性和用例	低成本配件/耗材验证 数据加密	低成本配件/耗材验证 软硬件防克隆 / IP保护 密钥配置	节点 / 配件验证 节点到云端的鉴权 网络鉴权（令牌） 密钥配置	节点到云端的鉴权 网络鉴权（令牌） 使小型MCU支持TLS1.2, TLS1.3 安全引导 安全升级（OTA或DFU） 软件IP保护 用户数据的安全存储 配件鉴权 密钥配置	TPM 1.2协议 节点鉴权 IP网络安全 节点到云端的验证和登录 远程认证 通信数据加密/解密 通过FIPS 140-2认证 通过EAL4+认证标准	TPM 2.0协议 节点鉴权 IP网络安全 节点到云端的验证和登录 远程认证 通信数据加密/解密 灵活的加密方式 FIPS & CC Pending
加密算法	NIST AES128	NIST SHA256	NIST SHA256; ECC P256	NIST SHA256; ECC P256, AES128	NIST SHA1, SHA256, RSA 1024 – 2048	NIST SHA256, ECC P256, RSA 1024 – 2048
非易失性存储器	1.5 Kb	4.5 Kb	8.5 Kb	8.5 Kb	64 KB	256 KB
I/O接口	I2C, 单线	I2C, 单线	I2C, 单线	I2C, 单线	I2C, SPI	I2C, SPI
封装	2 pin 2x2, 2 pin 2x4, UDFN8, SOIC8 3-Contact (RBH)	UDFN8, SOIC8, SOT23-3, 3-Contact (RBH)	UDFN8, SOIC8, SOT23-3 封装 且引脚兼容	UDFN8, SOIC8, SOT23-3 封装 且引脚兼容	QFN32, TSSOP	UDFN8, QFN32, TSSOP
供应情况	量产中	量产中	量产中	量产中	量产中	SPI版本已量产 TCG rev.116

© 2019 Microchip Technology Inc. All Rights Reserved.

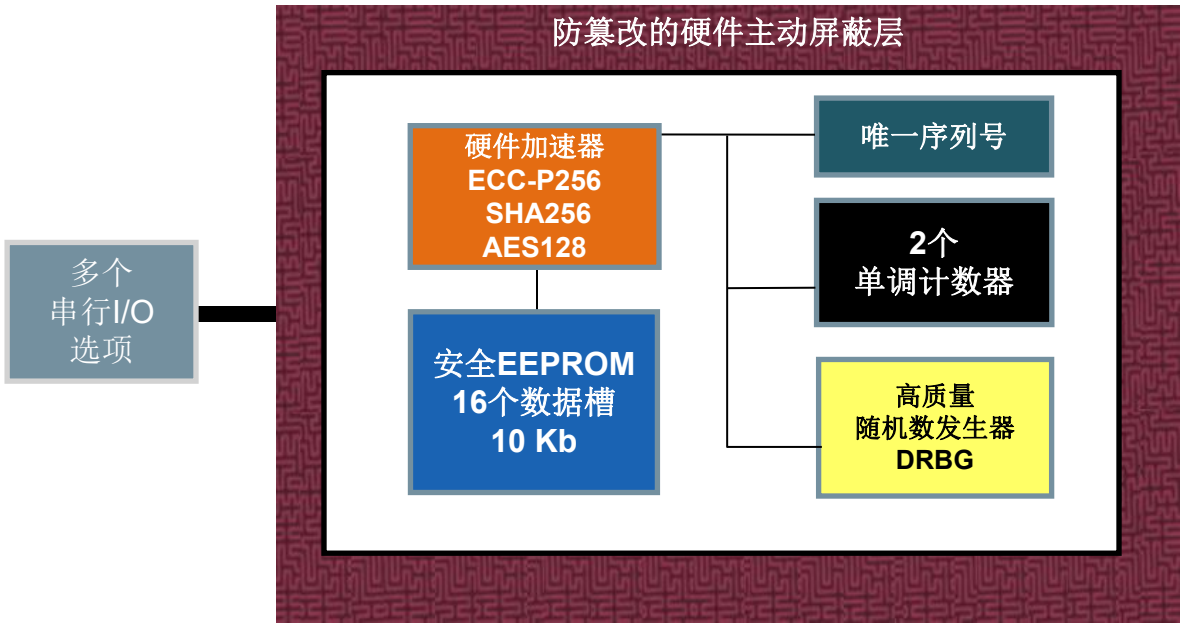
ATECC608A
用硬件防护来隔离密钥

ATECC608A可以在器件的整个生命周期中安全地存储密钥信息。

密钥是在器件内部安全生成的，并且生成过程基于符合NIST规范的“最佳级”随机数发生器（RNG）

所有关键的密码运算都在密钥所在的器件内执行：

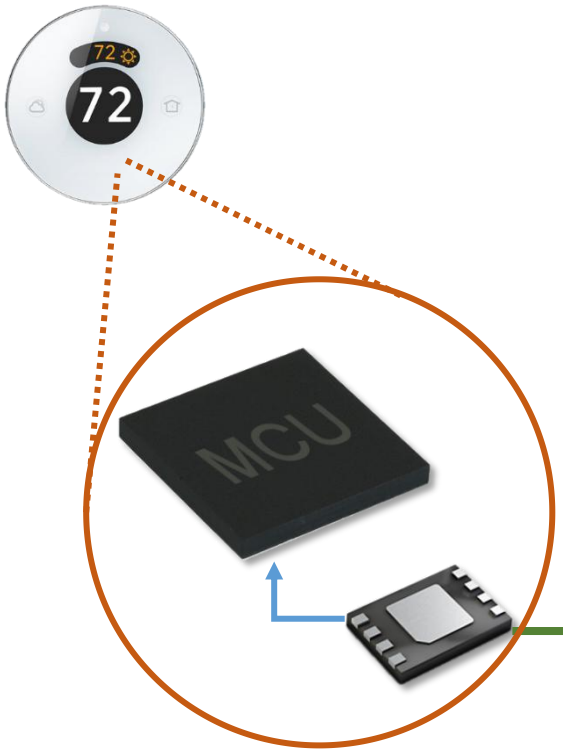
这样可以确保密钥和运算过程与外部严格隔离开，防止敏感数据外泄



- 与MCU/MPU相比，加密算法的硬件加速器执行更快，而且功耗更小
- 内部信息在EEPROM中被杂散和加密
- 每个器件都有唯一的72位序列号
- 用于控制使用次数的单调计数器
- 多个串行I/O选项：I2C或SWI

© 2019 Microchip Technology Inc. All Rights Reserved.

为IoT系统提供多层安全防护



ATECCx08A
安全协处理器

云端应用层

ECDSA – 数字签名验证：唯一性，
验证设备身份
设备安全引导/升级

网络传输层

ECDH – 会话密钥协商
TLS/DTLS 安全传输

链路层

安全数据存储 – 网络证书，
本地访问权限控制

© 2019 Microchip Technology Inc. All Rights Reserved.

灵活的预配置选项，简化资源预置流程

	TRUST&GO	TRUST FLEX	TRUST CUSTOM
预先配置	是	是	否
预先资源预置	是	是（灵活）	否
MOQ	10颗	2000颗	4000颗
开发时间	最少	较少	定制
复杂度	最低	较低	定制
安全密钥存储	JIL高	JIL高	JIL高
应用场景	TLS, AWS, GCP, 私有云 LoRaWAN™	TLS 鉴权 安全引导和升级 软件IP保护 信息加解密 主机对外设的鉴权	任何定制化的应用场景

© 2019 Microchip Technology Inc. All Rights Reserved.

提供可信任平台设计套件

1 定义

将使用场景
与配置相映射

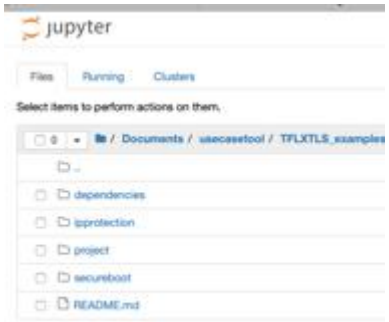
场景配置工具

2 原型设计

Python
可执行文件教程

Jupyter Notebook

3 开发



每个使用场景都有
C代码项目

适用于任何 IDE

4 发布

生成
加密的交换文件

加密交换

© 2019 Microchip Technology Inc. All Rights Reserved.

硬件开发工具

DM320118

可信任平台USB工具包

- 直接原型设计
- 通过USB连接PC主机（使用Python Jupyter Notebook教程）
- 或板上SAMD21，带有调试器

DT100104

ATECC608A可信任平台评估板

- 支持：
  - Trust&GO,
  - TrustFLEX,
  - TrustCUSTOM
- MikroBUS™公插槽

AT88CKSCKTUDFN

CryptoAuthentication™插座工具包

- uDFN8插座
- SOIC8插座
- Xplain PRO尺寸

Mikroe.com插座

- UDFN和SOIC
- 与XPRO插座板具有相同功能
- MikroBUS™公插槽
- Mikroe.com售卖

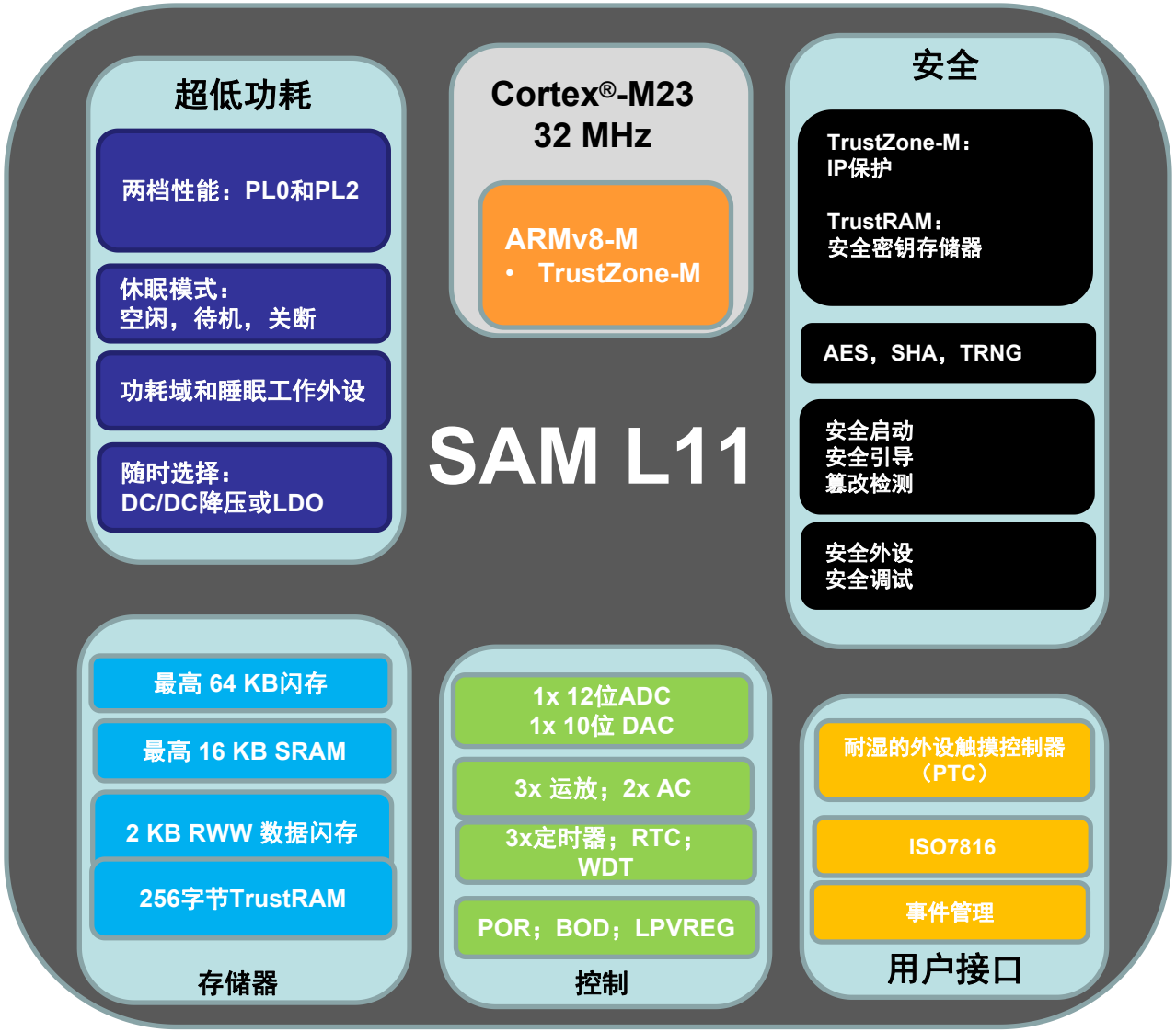
© 2019 Microchip Technology Inc. All Rights Reserved.

Microchip带安全特性的MCU：集内核、性能和安全特性为一身

32-bit MCU Product Family	Description	CPU Frequency (MHz)	Secret Key / Symmetric Crypto (AES, 3DES)	Public Key / Asymmetric Crypto (RSA, DSA, ECC)	Hash / Integrity Check Monitor (SHA)	HW Root of Trust / Secure Boot (Immutable ROM)	Secure Update / Secure Bootloader	Tamper Detection	TRNG	Secure Key Storage	Key Provisioning	Hardware Isolation / IP Protection (Trust-Zone)
SAM L10	ARM® Cortex-M23, 16-64KB Flash	32						√	√			
SAM L11	ARM® Cortex-M23, 16-64KB Flash	32	√		√	√	√	√	√	√	√	√
SAM L21	ARM® Cortex-M0+, 32-256KB Flash	48	√						√			
SAM L22	ARM® Cortex-M0+, 64-256KB Flash	48	√					√	√			
CEC1702	ARM® Cortex-M4F, 480K SRAM	48	√	√	√	√	√		√	√	√	
SAM 4E	ARM® Cortex-M4F, 512-1024KB Flash	120	√					√				
SAM 4L	ARM® Cortex-M4, 128-512KB Flash	48	√						√			
SAM G	ARM® Cortex-M4F, 256-512KB Flash	120						√				
SAM D5x / E5x	ARM® Cortex-M4F, 256-1024KB Flash	120	√	√	√		√	√	√			
PIC32MZ EF	MIPS M-class, 512-2048KB Flash	200	√		√				√			
PIC32MZ DA	MIPS microAptiv, 1024-2048KB Flash	200	√		√				√			
SAM S7x / E7x / V7x	ARM® Cortex-M7, 512-2048KB Flash	300	√		√		√	√	√			

© 2019 Microchip Technology Inc. All Rights Reserved.

SAM L11
安全MCU / 超低功耗



- Cortex®-M23
  - 具有TrustZone® 功能的ARMv8-M内核，
  - 硬件除法器
  - 增强型MPU
- 存储器
  - 64 KB闪存
  - 16 KB SRAM
- 超低功耗
  - 工作电流：
    - ~25 µA/MHz
  - 待机电流，数据仍保持着
    - ~600 nA
  - 关断模式，电流为100 nA
- 安全功能
  - TrustZone-M
  - 安全启动和引导
  - 安全密钥存储器
  - 篡改检测
  - 数字主动防护
  - FIPS认证的加密
  - 支持安全密钥资源预置

© 2019 Microchip Technology Inc. All Rights Reserved.

SAM L10/11目标应用

超低功耗应用

- 从待机（<0.6 µA）到完全唤醒（<25 µA/MHz）只需2.6 µs
- 外形小巧、功耗极低，非常适合电池供电的节点
- 灵活的电源管理，可在功能与功耗之间实现完美平衡
- 低功耗外设可在休眠期间运行

简单的可穿戴设备、用户界面和传感器

- 电容式触摸功能，支持在潮湿环境下工作，响应速度更快且抗噪声能力强
- 可支持数字和低功耗模拟传感器接口
- 可配置的SERCOM用于传感器、RF等，支持I²C/SPI和LIN总线
- 内置的安全功能可覆盖到数字传感器和用户界面控制器

传感器节点和控制

- 基于LoRa、SigFox和BLE的物联网边缘设备
- 在休眠模式下工作的超低功耗模拟外设可检测传感器的变化
- 内置运算放大器可用于低功耗模拟传感器
- I²C和SPI主模式适用于连接外部数字传感器，并且I²C和SPI也支持从模式

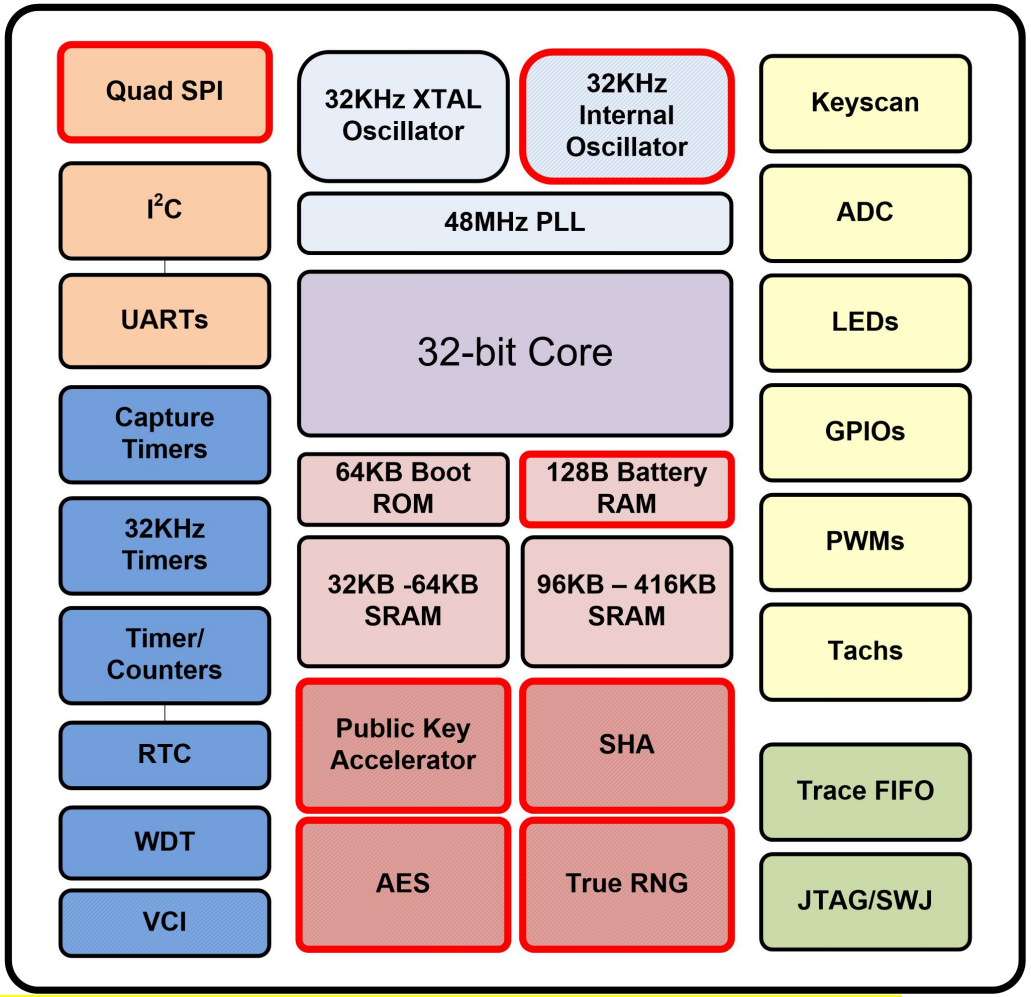
安全和沙盒化

- TrustZone®-M用于IP保护和密钥存储
- 加密加速器用于哈希运算/加密、安全引导和验证
- 沙盒化：用户应用代码无法更改或单步执行经安全防护的软件
- 提供了对开发人员友好的开发环境

© 2019 Microchip Technology Inc. All Rights Reserved.

CEC1702加密嵌入式控制器

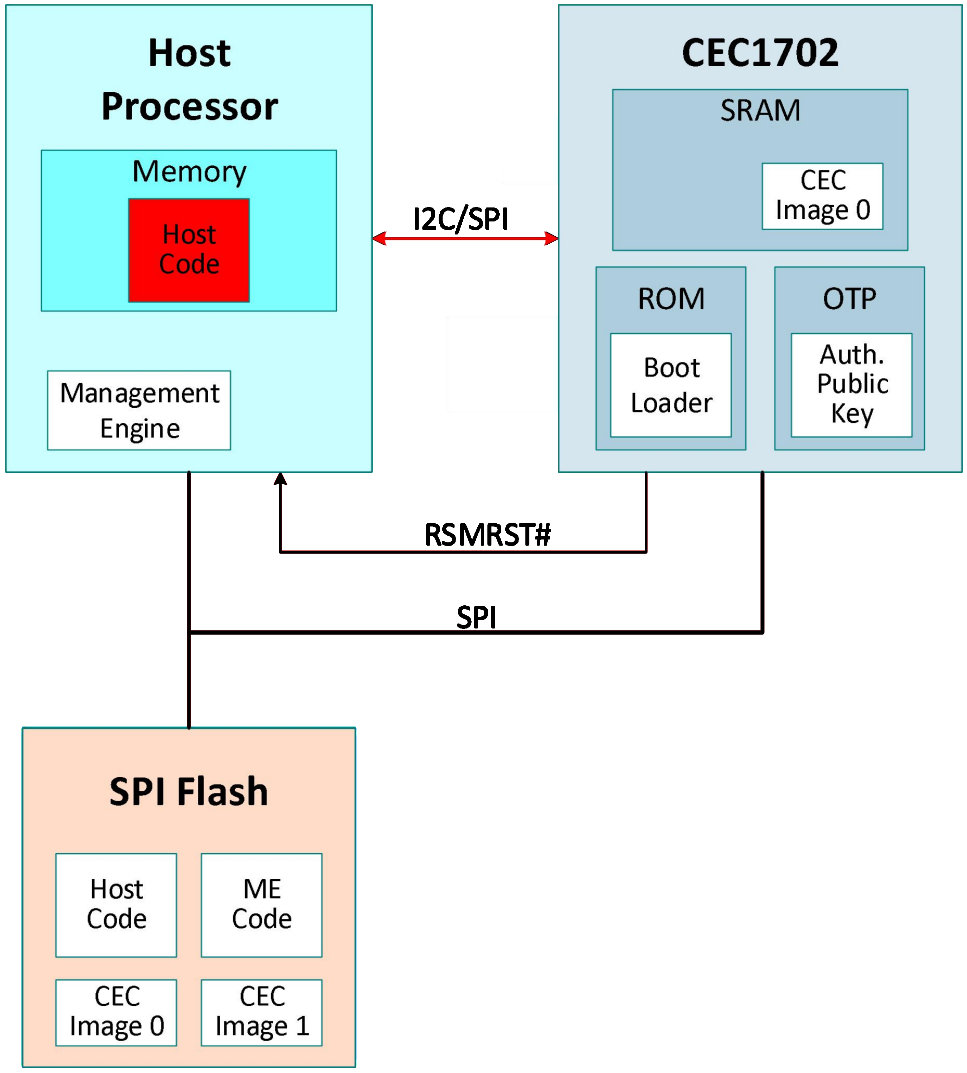
- **产品特性：**
  - ARM® Cortex®-M4F单片机
  - 480 KB SRAM：代码 + 数据
  - 64 KB引导ROM
  - 稳健的硬件加密密码套件：
    - 真RNG
    - AES128、AES192和AES256
    - SHA-1、SHA-256和SHA-512
    - RSA-1024至RSA-4096
    - ECC-192 ~ ECC-640，Curve25519
    - ECDSA、EC-KCDSA和Ed25519
  - 2.5 Kb用户可编程OTP
- **典型应用：**
  - 应用处理器的安全引导
  - 工业IoT的联网设备
- **独特之处**
  - 安全启动提供不变的信任链



CEC1702可用于安全引导和对CEC1702或系统中的其他器件上后续加载运行的代码作鉴权——身份验证（现场升级）

© 2019 Microchip Technology Inc. All Rights Reserved.

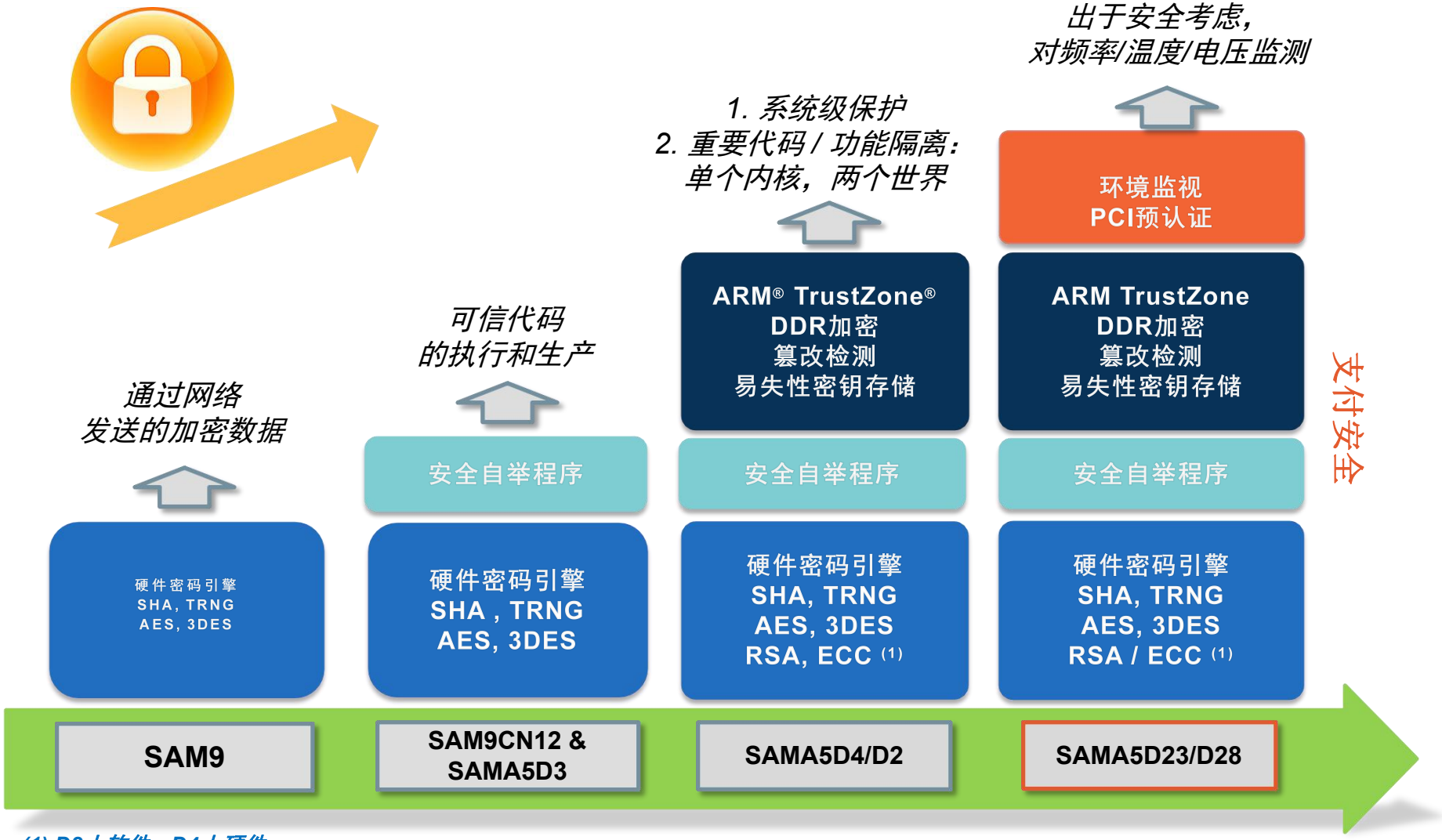
基于硬件的安全引导



- 受信任的不可变代码（引导装载程序）驻留在CEC1702 ROM中
- 由OEM使用私钥签名的应用程序代码存储在SPI闪存中（CEC映像0和1）
- 由私钥签名的主机代码也存储在SPI闪存中
- 在上电阶段，受信任的代码：
  - 将主控制器保持在Reset状态
  - 将CEC映像0加载到SRAM中
  - 使用存储在CEC1702 OTP内存中的公钥进行身份验证
  - 允许执行CEC代码
- 然后，CEC代码使用CEC代码中的公钥对SPI中的主机代码进行身份验证
- CEC代码将主机处理器从Reset中释放
- 然后，主机处理器从SPI加载并执行其经过身份验证的代码
- 主机处理器也可以使用CEC1702作为密码协处理器

© 2019 Microchip Technology Inc. All Rights Reserved.

MPU32 安全性概述



(1) D2上软件，D4上硬件

© 2019 Microchip Technology Inc. All Rights Reserved.

使用Microchip的整体方案快速接入云架构

整体解决方案

amazon web services

Google Cloud

Microsoft Azure

LoRa

AWS IoT Core examples

Microsoft Azure examples

Network operators: The Things Industries & Actility

Microchip.com/Trust&GO coming soon: microchip.com/Trust&GO-LoRa + AWS

Azure examples coming soon: microchip.com/TrustFLEX-Azure

SAMG55 (Arm® Cortex®-M4), Raspberri Pi, Atmega4809, PIC24

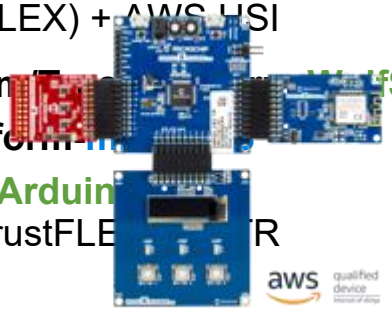
Microchip.com/ATECC608a-HSI

SAMA5Dx + Greengrass + ATECC608a (Trust&GO or TrustFLEX) + AWS HSI

所有代码包包含
Other participating partners addressing

Wiki user manual

Turnkey code examples



Complete HW solutions

© 2019 Microchip Technology Inc. All Rights Reserved.

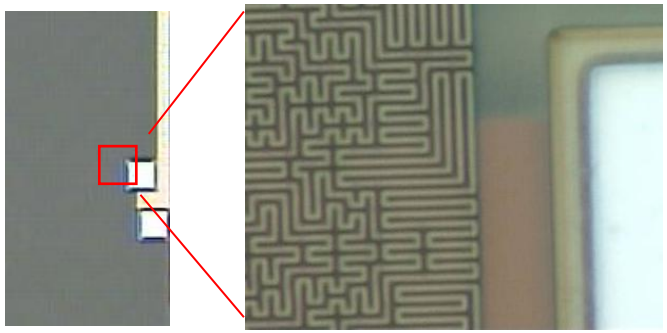
总结：Microchip安全方案的优势

总 结

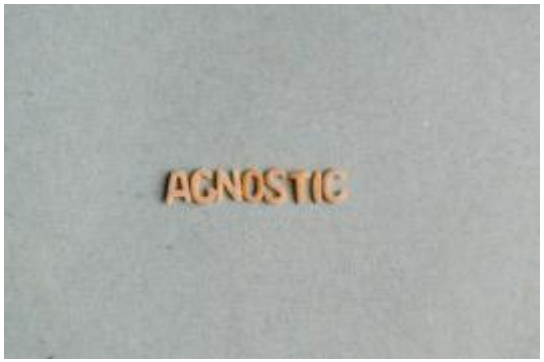
典型应用场景很容易
导入到新产品

提供简单的工具集
和完整的系统方案
助您快速完成开发

利用电子商务网店
带来更简便的购买流程



晶元级的硬件安全保护，
让秘密固弱金汤



与架构无关——可工作于任何云、
任何PKI、任何控制器和任何连接

*PKI: public key infrastructure

© 2019 Microchip Technology Inc. All Rights Reserved.

谢谢！