安全产品

术语表

世界级的嵌入式安全解决方案确保对每个系统设计的信任

当今，安全的关键在于信任。Microchip安全产品使“信任”可以简便地嵌入任何系统。除了使用安全解决方案来防止对您的产品或通过您的产品发起的恶意攻击之外，还可以使用加密和身份验证来改善客户体验，通过防止您的产品被克隆来保护您的品牌乃至收益。灵活性、先进的功能、创新的高成本效益架构，以及超安全的硬件防御机制使Microchip基于硬件的安全器件成为通过设计增添信任的一种理想方式。

从基于硬件的加密伴随芯片到带集成安全组件的单片机和微处理器，Microchip提供各种各样的解决方案。

- **CryptoAuthentication™库**——为您提供成本效益极高且易于设计的微型超安全硬件身份验证功能。
- **可信平台模块**——Microchip可信平台模块（TPM）通过单个器件为个人电脑与平板电脑以及基于嵌入式处理器的系统提供强大的基于硬件的公钥（RSA）安全性。
- **CryptoMemory® IC**——Microchip CryptoMemory IC系列为需要全面数据保护的应用提供一系列成本效益高、安全性高的电可擦除可编程只读存储器芯片（EEPROM），提高主机端的安全性。
- **CryptoRF®器件**——Microchip的13.56 MHz RFID CryptoRF器件系列采用64位嵌入式硬件加密引擎，支持双向身份验证，最高具有64 Kb的用户存储器。
- **应用处理器的安全引导**——CEC1302和CEC1702是基于Arm® Cortex®-M4的全功能单片机，为保护应用处理器的引导而设计，在单个封装中提供具有完整硬件加密加速器功能的解决方案。这些产品也可以在嵌入式应用中用作独立MCU。
- **安全SAMA5D2 MPU**——SAMA5D2 MPU系列通过设计确保安全，设立了保护嵌入式应用的标准。Arm TrustZone®、硬件加密、安全存储器以及多种监视机制可检测或防止入侵企图。它已获得PCI预认证，是金融交易（如POS终端）的首选解决方案。

术语	定义
高级加密标准(AES)	一种快速对称密钥算法，分块长度为128位，密钥长度为128、192或256位，基于代换 – 置换网络。
Alice、Bob和Eve	Alice是赋予第一个用户的名字，Bob是第二个用户的名字，Eve是赋予窃听者（黑客）的名字。
Arm® TrustZone	嵌入ARM Cortex®-A处理器（自ARMV6架构以来）和ARM Cortex-M处理器（自ARMV8M架构以来）中的电路，使软件可以拆分为可信部分和普通部分。
非对称密钥算法	一种使用私钥和公钥进行加密和解密的加密算法。
非对称密钥加密	使用一个密钥进行签名或加密，使用另一个密钥进行验证或解密的加密技术。
攻击	试图破解在安全服务中实现的加密方法。它包括穷举、中间人和明文攻击。
攻击面	系统潜在的安全漏洞。
身份验证	确保事物与其所声称的一致。例如，它确认报文的来源来自特定发送者。
分块加密算法	一种对称密钥算法，通过将报文分解为固定大小的块并对每个块进行加密来实现对报文的加密。
穷举攻击	这种攻击的特点是系统性地猜测每个密钥，并使用这些密钥来破译密文。 密钥长度越长，攻击需要消耗的时间和计算能力就越多。
证书颁发机构(CA)	颁发数字证书并在一个“信任链”中提供“信任锚”或“信任根”的实体。
信任链	一种证书或签名结构，使“信任锚”可以保证结构中其他成员的可信度。称之为“链”是因为每层的可信度都由信任锚的前一个层保证。
校验和	分配给文件的一个值，之后进行测试后可确认是否对原始文件进行了任何恶意更改。
密码	一种加密解密算法。通过该算法的明文会变为密文。
密码块链接(CBC)	分块密码操作模式，每个密文块取决于之前的密文块。对第一个块使用初始化向量（IV），以确保每个报文唯一。
Curve25519	用于ECDH的特定椭圆曲线，提供128位安全性，是速度最快的ECC曲线之一。也被称为ED25519和Edwards曲线。
数据加密标准(DES)	一种使用56位密钥的对称加密算法。三重DES（3DES）会对每个块应用三次DES。3DES更安全，因为它使用3个不同的密钥，相当于168位密钥。
解密	密文恢复为原始数据（明文）的变换。
Diffie-Hellman	一种非对称密钥协议算法。通常，两个实体交换一些公共信息，然后通过安全的数学算法将它们与自己的私钥组合，生成一个共享会话密钥。
数字证书	一个电子文档，将一些信息片段（例如用户的身份、公钥和/或数字签名）绑定起来。
数字签名	将计算得到的数字与报文和签名者相关联的非对称密钥算法。根据算法，计算得到的数字使签名者可以解决报文的认证、完整性和不可抵赖性。
数字签名算法(DSA)	一种使用公钥/私钥对中的私钥创建数字签名的非对称密钥算法。签名通过关联的公钥验证。
电子密码本(ECB)	一种分块密码加密模式，将每个明文块单独加密为密文块。
椭圆曲线	满足以下方程的数学结构，其中的x和y为变量，a和b为常量：$y^2 = x^3 + ax + b$（在域GF(p)中），$y^2 + xy = x^3 + ax^2 + b$（在域GF($2^n$)中）。
椭圆曲线加密(ECC)	一种基于椭圆曲线约束的非对称密钥算法。通常与Diffie-Hellman（ECDH）和DSA（ECDSA）结合使用。
椭圆曲线Diffie-Hellman(ECDH)	椭圆曲线加密和Diffie-Hellman密钥交换结合使用，生成一个共享密码。
椭圆曲线Diffie-Hellman临时(ECDHE)	使用临时密钥实现的ECDH。在使用密码之后，会将它与临时密钥对一起销毁。这种短暂密码是实现完全向前保密的基础。

术语	定义
椭圆曲线数字签名算法(ECDSA)	ECC和DSA结合使用。
加密	使用一种算法将原始数据（明文）转换成不可理解的数据（密文）。
熵	混乱程度的度量。加密中使用的随机数需要极高的熵。
联邦信息处理标准(FIPS)	美国政府制定的数据保护相关标准。
黑客	试图攻破数据安全措施的人。
哈希函数	常称为报文摘要算法。用于产生报文摘要的算法。常用的哈希函数包括MD2、MD4和SHA。
HMAC	基于密钥的哈希，用于生成报文认证代码。
识别	一个用户识别另一个用户的过程。
初始化向量(IV)	用于初始化对称密码泵的初始数据块，从而现在总是从完全相同的状态开始实际加密。
密钥	在加密函数中使用的一个参数。密钥类型包括私钥、公钥、秘密密钥和会话密钥。
密钥协议	系统中的两个实体达成公用密钥的过程。
密钥功能	关于密钥的常见功能，包括扩展、生成、管理、恢复和撤销。
密钥对	相应的公钥和私钥组成的对。总是存在于非对称密钥加密。
密钥生成方案	在密钥空间内的密码块中创建子密钥的算法。
密钥空间	密码系统中所有可能密钥的集合。
报文认证代码(MAC)	使用MAC算法和对称密钥进行的明文转换，提供身份验证和数据完整性，也称为MIC。
MAC算法	用于产生MAC的算法。常用算法包括HMAC-MD5、HMAC-SHA-1和HMAC-SHA-512。
中间人攻击	黑客居于各通信方之间并收集所有数据的攻击。
报文摘要	可提供数据完整性的转换。通过使用哈希算法来生成。该算法接受可变长度的数据，并将其转换为固定长度的数据。也称为指纹。
美国国家标准与技术研究院(NIST)	美国政府负责制定加密安全标准的部门。
一次性随机数据	使用一次的数字。一次性随机数用于确保操作的唯一性。这种唯一性可阻止重放攻击，使反向计算密钥不可行。
一次性密钥	也称为完美密码，是一种将明文报文与等长密钥进行组合的加密算法。通常与XOR函数配合使用。它是现有的唯一被认为在数学上不可攻破的密码。
完全向前保密	保护过去的会话，防止未来泄漏密钥或密码。亦称：向前保密。
明文	传输的无加密保护的数据。也称为明文（cleartext）。
私钥	该术语取决于上下文。如果讨论的是对称加密，则私钥与秘密密钥（共享密钥）同义。在非对称加密中，私钥是公钥/私钥对中保密的那一个。
伪随机数(PRN)	看似随机但实际上由特定函数和种子值决定的数字。PRN通过PRNG（PRN发生器）创建。
公钥	非对称加密中的通用密钥。
公钥基础设施(PKI)	创建、管理、分发、使用、存储和撤销数字证书以及管理公钥加密所需的一组角色、策略和过程。
随机数	合理预测比意外预测的几率更低的数字。由随机数发生器（RNG）产生。

术语	定义
信任根	一个权威实体，假定其可信，但不能衍生。也称为信任锚。
RSA	一种可以加密数据以及创建和确认数字签名的非对称密钥算法。
盐值	在密钥中添加的一串随机或伪随机位，以提高攻击的复杂度。
秘密密钥	对称加密中用于加密和解密的共享密钥。
密码共享	将一个密钥分拆为许多片断，从而使用户需要所有片段才能使用该密钥。
安全引导	验证特定硬件部分仅使用可信固件进行引导的过程。
安全远程密码(SRP)	一种安全协议，它使窃听者无法在没有其他各方参与的情况下通过穷举猜出密码。
种子	一个随机数字序列，用于获得更多的随机数。
会话密钥	仅在用户之间的通信期间使用的密钥。
安全哈希算法(SHA)	为每个输入生成唯一哈希值的报文摘要算法。
SHA-1	一种SHA算法，其强度不再被认为足以防御当今黑客。该哈希函数使用160位的哈希值。
SHA-2	取代SHA-1。该哈希算法的工作方式相同，但产生更长且强度更高的哈希。主要有四种变体：SHA-224、SHA-256、SHA-384和SHA-512。缩写词末尾的数字表示所产生哈希的位长度。
SHA-3	SHA系列的最新版本。不同于SHA-1和SHA-2，它采用被称为海绵构造的新结构，其中的数据被“吸收”到海绵中，然后结果被“挤”出来。其结果是基于置换的哈希。
共享密钥	在对称密钥加密中用户共享的密钥。
共享密码	只有通信双方知晓的数据片段。
边信道攻击	基于密码系统的物理实现信息的任何攻击。可用于破解系统的信息包括时间信息、功耗和电磁泄漏。
签名/验证	请参见数字签名算法。
对称密钥算法	一种使用的密钥为系统中的实体之间共享的加密算法。
对称密钥加密	采用对称密钥算法的加密技术。
防篡改	不可能或几乎不可能从中提取信息的硬件设备。
传输层安全(TLS)	在Web服务器和浏览器之间创建加密链路的标准安全技术。其前身被称为安全套接字层（SSL）。
信任锚	信任锚是一个权威实体，假定其可信，但不能衍生。亦称：信任根。
可信平台模块	由可信计算组织制定的针对集成图形密钥的单片机的国际标准。
验证	一个用户验证另一个用户是否为其所声称对象的身份验证子过程。