256 位密钥：足够长了吗？

摘要

作者：Kerry Maletsky

大多数加密算法、加密设备或加密协议的安全性都受到其密钥或其他机密信息大小的限制。本白皮书介绍如何使用加密技术对产品（无论是实体产品还是固件逻辑模块）进行身份验证，以及需要使用多长的密钥才能从容应对攻击者或其他安全威胁。

身份验证

使用最新技术开发产品的成本非常高昂。而开发成本越高，克隆产品的诱惑也越大。目前，假冒伪劣商品占全球贸易的 1%至 5%，并且正以惊人的速度不断增长。

由于克隆产品没有保护声誉的需要，因此质量和性能通常不佳。克隆产品可以绕过开发过程，在产品安全性和可靠性上偷工减料，从而降低产品成本，获得更大利润。

- 如果墨盒出现故障，可能会令人恼火。
- 如果因为使用假冒伪劣电池而导致最终产品损坏，可能会损失惨重。
- 如果医疗耗材不符合标准，可能会危及生命。

另外，微处理器固件也存在安全隐患。产品中通常会有一些功能专门用于保护最终用户的固件免遭未经授权的下载，但黑客们一直都在想方设法破解这些功能。尽管将手机开放给其他服务提供商似乎很有吸引力，但同时也将面临着手机被安装恶意软件的风险，这些恶意软件可能会窃取最终用户的个人信息，甚至对手机本身造成损坏。

假冒伪劣产品或软件可能对最终用户造成以下危害：

- 损害原始设备制造商（Original Equipment Manufacturer，OEM）的声誉。
- 增加产品责任。
- 增加维护和保修成本。
- 影响未来销量。

如何对产品进行身份验证

OEM 一直都在努力通过各种方式保护自家产品的安全以及防止假冒伪劣产品。对产品进行身份验证有许多常用的方法：

来源

如果产品的卖家和托运人值得信赖，则可以使用这种方法进行身份验证。潜在的问题很容易发现：

- 真正安全的托运（例如，使用装甲卡车托运且每时每刻都能完全控制产品）通常十分昂贵，极少有人使用。尽管产品也有可能在托运人不知情的情况下被调包，但这种情况并不常见。
- 即使是信誉良好的卖家也有可能无法完全掌控他们的供应链，因为可能有人假借他们的名声售卖假冒伪劣产品。
- 我们假设有一些卖家在售卖假冒伪劣产品，比如街头小贩以 15 美元售卖原价 100 美元的棒球衫。但是，这些产品并不是街头小贩生产的。这些假冒伪劣产品的制造商还有哪些其他的销售渠道呢？

物理属性

对于具有独特外形的产品（如计算机电池、打印机碳粉盒或真空吸尘器袋），我们通常认为只要标签看起来是真的、上面的徽标没有问题并且产品能够正常工作，那就是正品。

- **“眼见为实”。**
  只要计算机正常工作、打印机正常打印或者真空吸尘器正常清洁卫生，我们通常就会认为这些产品是正品，尽管我们知道克隆产品也可以做到，而且仿制标签十分便宜。
- **我们可能永远也不会去查明真相。**
  实际上有多少人真的：
  - 会去数一数他们更换的碳粉盒打印了多少页？
  - 能分辨出通过真空吸尘器袋的颗粒的大小？

全息标签

全息标签在服装和许多其他零售产品中很常见。这类标签看起来很高级，似乎很难使用我们熟悉的设备进行翻印，但是当您在搜索引擎中输入“全息印刷”时，您就会发现满屏都是这类翻印公司的小广告。

- 还有一种增强防伪的方法是在金属标签上刻印序列号；但这类标签的仿制难度还没有全息标签高。

密码

使用密码登录计算机或访问网站上的帐户/信息是一件很普遍的事情。但密码也经常用于在基于控制器的系统内部验证单独的设备、电路板、消耗品或网络设备。此外，密码还可用于控制对系统的特殊访问，以便进行配置和维护等。共享机密信息加密密钥是密码的“近亲”，二者具有相同的优缺点：

- 接收系统上通常没有位置可以安全地存储预期密码，因此只要攻击者可以访问该系统，便可以从 EEPROM、闪存或其他非易失性器件中提取密码值。
- 通常，攻击者很容易找到一种方法来监视正在使用的系统，当某个系统元件中传递密码时，攻击者便可发现密码。攻击者也可能会记录整个会话，然后过一段时间再重放一遍，以此将第一个用户获得的利益收入囊中。
- 此类安全性还有一种更为复杂的版本，即在消耗品中包含序列号的公钥签名。主机设备无需存储任何机密信息即可验证该签名。但由于序列号和签名通常都存储在不安全的设备中，因此可以轻松读取它们并将其复制到克隆设备中。

智能卡

一些卫星电视、有线电视或其他媒体的提供商使用智能卡来对网络用户进行身份验证。用户需将智能卡插入机顶盒才能访问媒体。智能卡通常十分安全，只是不能完美适用于所有应用。

- 智能卡的尺寸不小，如果要插入的设备太小、需要在潮湿或脏乱的环境中使用，或者最终用途（许多消费品）要求不能丢失任何部件，那么这种方法就不可行。
- 每个智能卡的成本为 5 美元。这对于售价不到 100 美元的最终产品来说太高了。
- 甚至系统总成本也会变高，因为除了支持 ISO 7816 接口所需的电子元件和智能卡本身之外，还必须配备物理读卡器插槽和连接器，这些都是需要成本的。

低成本的加密身份验证补救技术

硬件身份验证器件已经推出一段时间了，但直到最近才终于能够以经济易用的形式将可靠、稳健的加密技术应用到基于微处理器的典型应用中。几乎所有安全器件都包含某种机密信息以及加密处理元素。一般情况下，绝对无法读取到器件中的机密信息。机密信息会通过一种协议与输入的数据相结合，该协议能够在不泄露机密信息的情况下证明机密信息的存在。

加密器件通常配备有线接口或无线接口，功能也日益强大，这样可以增加伪造者破解任务的难度。有线器件既可以与其他系统元件一起焊接在电路板上，也可以安装到消耗品上并通过触点连接到系统。无线RFID 器件不需要触点，是应对严苛环境的理想选择。

这些身份验证器件通常包含一个序列号，与其他类型的序列号存储方案相比具有众多优势：

- 序列号由器件制造商编程到芯片中，因此可以更改。
- 序列号可以加密连接到设备上无法读取或复制的密钥。攻击者需要同时破解序列号和密钥才能伪造设备。

- 器件可以提供一种方法将来自主机的动态随机质询与序列号相结合。这种解决方案要出色得多，不像前文所述的静态签名机制那样容易被复制。

Microchip CryptoAuthentication™系列器件是同类器件中的最新产品，其中集成了依托安全器件悠久历史沉淀开发而成的安全功能，以一种前所未有的方式将安全性和易用性集于一身，同时成本还低于现有身份验证器件。

CryptoAuthentication 系列器件：

- 使用 SHA-256 哈希算法，以避免任何已知的算法弱点。
- 在整个内部电路上使用完整的有源金属屏蔽层。只要攻击者将屏蔽层中的任何电线切断或短路，器件就会停止工作。
- 使用内部时钟和电压生成功能。
- 使用全加密存储器。
- 使用篡改检测。
- 使用完全安全的生产测试方法。

该系列器件可凭借现代工艺技术集成在小于 2 mm x 3 mm 的 SOT23 封装中。这种小型封装足以集成到大多数空间受限的便携式系统中、集成到电池组中或者安装在现有 PC 板上（完全不会增大尺寸）。

CryptoAuthentication 系列的所有成员均包含：

- 保证惟一的 48 位序列号。
- 用于验证序列号并非假冒伪劣产品上的简单仿制序列号的适当加密协议。

单线接口简化了器件的机械连接，同时减少了主机单片机上所需的 GPIO 或 UART 资源数量。完成加密操作后，自动休眠模式会将待机电流降至 100 nA 以下。CryptoAuthentication 器件采用直接质询-响应机制，同时搭配使用商业和开源软件库广泛支持的算法，可简化编程要求。

每个加密器件的两个重要特性分别是密钥的长度和算法的能力。不难想象，密钥越长，安全性越高——但是，多长算过长？人们往往会认为最新的机密信息算法就是最好的算法，但“不公开即安全”（Security Through Obscurity）通常非常危险。加密专家更喜欢广为人知且多年来已被许多聪明人士分析过的算法。以下部分将更为详细地讨论这些概念。

256 位密钥是否足够长？

随着计算能力的迅速提高，加密器件中的密钥长度得到了越来越多的关注。个人计算机通常搭载时钟频率为 4 GHz 或更高的四核处理器，因此通过尝试破解具有数十亿种可能性的密钥可谓轻而易举。这些攻击通常称为离线攻击，因为攻击者并不使用主机或客户端系统来尝试每种可能性，而是使用外部计算机模拟身份验证器件的计算以猜测存储的机密信息，从而尝试生成与真实系统上记录过一次的内容相匹配的位序列。

以最简单的蛮力攻击为例，攻击者首先获取全部或部分明文报文及其对应的加密报文（通过攻击者想要破解的密钥实现的加密），然后连续尝试每种可能的密钥，直到找到那个创建已获取加密报文的密钥。如果密钥为 n 位，则在 2n - 1 次尝试后，攻击者会有 50%的几率找到正确的密钥。攻击者只需要 2n 次即可尝试完所有可能的密钥，保证会找到密钥。

对于这种蛮力攻击，惟一的保护措施就是选择一种算法让使用的密钥长度足够长，这样仅仅是尝试大部分的可能性就需要花费特别长的时间。由于计算能力呈指数级增长，10 年前足够长的密钥现在已不够复杂。以下是一些广为人知的蛮力攻击成功案例：

- Xilinx®的 64 Virtex-5 FPGA 阵列不到一个小时就可以成功破解 48 位密钥。广泛用于保护电子钱包内容的 MIFARE®加密存储器使用的就是 48 位密钥。
  请参见 http://www.usenix.org/events/sec08/tech/full_papers/nohl/nohl.pdf。
- 美国于 1976 年采用的官方加密标准“数据加密标准（Data Encryption Standard，DES）”使用更长的 56 位密钥。但是，当时仍有计算机可以通过蛮力攻击在不到一周的时间内破解密钥。
  请参见 http://en.wikipedia.org/wiki/EFF_DES_cracker。

尽管采用 56 位以上密钥长度算法的商用设备尚无被蛮力攻击破解的报告，但预计随着计算能力的提高，采用更长密钥的算法终将被破解。撰写本文时，美国政府推荐政府部门采用 128 位密钥的高级加密标准（Advanced Encryption Standard，AES）。撇开 AES 中的任何数学弱点（如果存在）不谈，政府坚信如此长的密钥在未来几年内是无法被破解的。但计算能力每 18 个月或每两年就会翻一番（见 http://en.wikipedia.org/wiki/Moore%27s_law），128 位密钥终将会被蛮力攻击破解。

因此，一些系统设计人员会寻求更长的密钥，以确保他们当下设计的系统在未来的整个生命周期内都能够保持安全。换句话说，即使黑客们未来可以使用更大更快的计算机也无法破解。目前，所有密码学家一致认为 256 位的密钥足以应对穷举攻击。那么，2^{256} 到底有多大呢？

下面给出了一些大数字的估计：

- 2^{66} = 地球上的沙粒数量。
- 2^{76} = 宇宙中的恒星数量。
- 2^{79} = 阿伏伽德罗数。12 克煤中的碳原子数量。
- 2^{96} = 一立方米水中的原子数量。
- 2^{190} = 太阳中的原子数量。
- 2^{255} = 破解该器件中的密钥所需尝试的次数。

美国国家安全局（National Security Agency，NSA）等资金雄厚的实体呢？他们能否制造一台机器来破解 256 位密钥？假设他们能够制造出一台理论上的纳米计算机，在一个边长为 5.43 nm 的立方体空间（即十个原子宽的硅晶格或包含 1000 个硅原子的晶体的近似大小）内每秒执行 10^{13} 条指令（原子振动的近似速率），并且假设这台计算机可以在 10 个周期内计算一次尝试，但就算是一台地球大小的计算机对 256 位算法进行蛮力攻击也得需要超过 10^{13} 年的时间（大约是地球年龄估计值的 58 倍）。

256 位密钥是否太复杂？

较长的密钥存在一些缺点，而这些缺点会在多个方面增加低成本身份验证器件的复杂性。

- **需要更多的内部存储空间来保存密钥和临时值：**
  大多数器件上最大的模块通常都是存储器阵列。密钥长度加倍通常意味着非易失性和易失性数据存储器的总空间也需要加倍，因此可能会增加器件成本。不过，随着器件中的线宽越来越小，存储单元的内核大小在器件总面积中的占比也越来越小，这样可以相应地降低成本损失。
- **逻辑门增多导致器件尺寸增大、成本增加：**
  通常，可以合理假设密钥长度加倍意味着实现模块的逻辑规模也需要加倍。如果依旧保持原先的逻辑规模，可能会导致计算时间增至两到四倍（具体取决于使用的算法）。不过，使用新一代技术实现晶体管更小的器件可以弥补这一缺点。
- **传输时间延长：**
  通常，质询和响应的长度与密钥相同。如果不同，则三者中最短的一个比另外两个更容易受到攻击。因此，密钥长度加倍意味着事务的传输时间也需要加倍。由于进行身份验证的频率不高（例如，仅在上电时需要），这种不利情况在整个方案中的影响较小。

密码学专家（和黑客）是富有创造力的一群人。尽管上一部分提到的 256 位密钥的破解时间令人望而却步，但目前已发现一些新的攻击程序可以将破解任务简化 2 倍、2000 倍甚至 2000000 倍。不过即便如此，仍可通过增加密钥长度、增大搜索空间来提高破解难度。因此，256 位密钥仍旧还是很难快速破解。

为什么不将哈希算法保密？

只要攻击者不知道算法，便无法进行蛮力攻击，因为即使他们知道密钥也无法计算输出。此类系统确实历经辉煌，但最近也开始逐渐退出历史舞台。

在某些情况下，尤其是在加密硬件的复杂性受到限制（可能是出于成本或功耗原因）和/或密钥存储机制不足的情况下，这仍然是一种合理的策略。RFID 标签就属于这种情况，这种标签不会消耗太多电流，而且成本也不会超过它们所保护内容（也许只是单程地铁票）的价值。

尽管如此，此类系统的使用还是越来越少，而采用广泛研究的开放算法构建的系统则越来越受青睐。这一切都要得益于半导体技术的进步，现在以更低的成本就可以生产出功耗更低的逻辑门。

算法很难保密：

- 恩尼格玛密码机是纳粹德国在二战期间广泛使用的一种加密设备，并且成功保密了数年之久，直到盟军夺取了密钥表和硬件。盟军的密码学家借此发现了恩尼格玛密码机的弱点，最终成功破解，为盟军提供了有力支持。

- 最初用于对欧洲 GSM 手机通话进行加密的加密算法一直受到保密协议（Non-Nisclosure Ngreement，NDA）的保护，但后来被一所大学在未获得 NDA 签名的情况下意外披露。加密算法很快被破解，手机被攻击的消息铺天盖地。
- MIFARE 器件中的加密算法（见上文）曾被另一所大学的团队从器件逻辑中成功提取出来，该团队后来合法购买了采用该算法的器件。他们在显微镜下研究逻辑，最终得出了其工作原理。

更优异的硬件设计策略（包括针对历史和预期安全攻击手段的对策）可以为采用加密算法的系统进一步延长未来的使用寿命。

基于哈希算法

加密哈希算法旨在将可变长度报文转换或压缩为固定长度字符串（称为摘要）。如果摘要对报文进行惟一标识，则摘要可以替代报文，从而缩短各种操作的计算时间。尽管许多算法可用于简单的哈希函数，但加密哈希算法有几个重要属性：

- 找到两条摘要相同的报文应该很难。如果确实存在两条这样的报文，则这种情况称为冲突。
- 即使给定摘要值，创建会产生该摘要的报文也应该非常困难。
- 通过报文创建摘要应该相对容易。

可以将报文摘要与密钥配合使用来执行一些加密操作，然后通过相应输出来验证报文的完整性。如果此验证代码的接收者知道密钥，则可以确信随代码一起发送的报文在传输过程中没有经过修改。

以这种方式使用时，此类验证代码通常称为报文身份验证代码（Message Authentication Code，MAC）。通常，附加到报文的 MAC 是搭配使用报文和密钥生成的。如果攻击者在不知道机密信息的情况下很难创建报文/MAC 对，即可认为 MAC 算法的能力很强。同样，攻击者应该无法通过匹配 MAC 的方式更改报文。哈希算法通常用于实现 MAC 算法。

SHA-1（安全哈希算法 1）和 MD5 哈希算法广泛用于加密目的。最近的数学分析表明，这些算法可能存在弱点。因此，它们在美国联邦政府推荐使用的算法套件中被 SHA-2（安全哈希算法 2）系列所取代。SHA-2 系列中最著名的算法是 SHA-256。

哈希算法的典型攻击策略是找到冲突——两条经哈希运算后得到相同摘要的报文。原因有两点：

1. 如果哈希算法用作报文身份验证或签名方案的一部分，则攻击者可以创建一条报文给发送者进行身份验证，但会替换接收者认为真实可信的另一条报文。这一点对攻击者非常有利。例如，只要攻击者可以更改订单上的送货地址，就可以在不付款的情况下收到货物。
2. 由于生日悖论（即在一组 n 个随机选择的人中，至少有两人生日相同的情况会达到一定概率）的原因（http://en.wikipedia.org/wiki/Birthday_paradox），这种攻击所需的尝试次数明显要少得多。如果摘要有 n 位，则只需对 2n/2 条随机报文进行哈希运算即可找到冲突。这相当于将位数减半！

因此，密码学家付出了巨大的努力寻求方法来创建两条冲突的报文。对于 SHA-1，尽管预期的攻击强度需要 280 次尝试，但当前最先进的攻击只需要 263 次尝试，可能在蛮力攻击的范围内。

生日悖论要求攻击者随机选择报文对。这似乎限制了其有用性。下面以电子邮件为例来说明为什么生日悖论非常强大。在简单的文本电子邮件中，我们看不到行尾的空格字符，但每行的末尾可能有一个可变数字。如果报文相对较长，则很容易看出如何能够生成大量报文，每条报文看似相同，但实际上都是惟一的。类似的概念也适用于图片附件——比如在我们眼中看起来相同的两张图片实际上在位级别上是非常不同的。

但是，出于一些具体的原因，蛮力生日攻击在大多数身份验证器件上都不起作用：

- 生日攻击通常的实现方式是计算所有看似相同的 2n/2 个版本原始报文的摘要以及 2n/2 个版本糖衣炮弹报文的摘要，并将第一组中的所有摘要与第二组中的所有摘要进行比较。由于在身份验证器件中，原始报文的所有位对于验证器是已知的（报文很短且格式固定），因此无法创建第一组，这会导致第二组的长度设为 2n。
- 将惟一 nonce 合并到报文中可以防止预先计算大量报文的摘要，否则这些摘要可能会与许多身份验证操作中每次记录的摘要进行比较。这是因为每条正确的报文都包含一个不同于先前所有“正确”报文的共享元素（nonce）。必须注意确保 nonce 不会被重复使用。

一些寻找冲突的攻击能够改变报文的长度，因此变得更容易。身份验证器件的固定长度报文属性可以抑制这些攻击。该属性还可以抑制长度扩展攻击，在此类攻击下，攻击者可以使用已知值扩展未知报文并为扩展后的新报文创建适当的摘要。将哈希算法与基于哈希算法的报文身份验证代码（Hash-based Message Authentication Code，HMAC）结构相结合也可以防止长度扩展攻击。

最新最好的算法是否足够？

使用最新最好的算法可以防止对算法本身的攻击。但这还不够。尽管授权系统遵循数据手册与这些安全器件进行交互，但攻击者可以访问超出正常操作范围的一系列选项，包括移除器件周围的封装并分析器件内的元件。

由于这些算法旨在防止安全器件被迫以明文形式披露其存储的密钥，因此必须将这些算法与一系列额外的保护措施相结合，以确保无法通过密码攻击以外的方式获取机密信息。

- **防攻击物理保护：**
  探测工作设备内部节点的设备被广泛用于攻击。身份验证器件应包括：
  - 覆盖内部节点的主动屏蔽层。
  - 缩小内部节点尺寸的最新工艺技术。
  - 多层内部互连，最好是三层以上。

  上述几点可以让微探测变得更加困难。
- **安全加密协议：**
  大多数算法都有已知的弱点，使用不当就会暴露。因此，必须以一种安全的方式在器件中使用算法。由于攻击者通常可以记录器件与真实系统之间来回传输的每一位，因此协议必须提供防重放保护。
- **极端环境：**
  例如，如果使用的时钟速率（过快）或电源电压违反数据手册规范，通常会导致器件发生故障。在某些情况下，攻击者可以利用这些故障从器件中读取机密信息。最先进的安全设计会通过控制环境或在检测到极端条件时关闭器件的方式来防止这种情况发生。
- **命令或 I/O 使用不当：**
  对于针对某些系统的堆栈溢出或存储器溢出攻击，许多程序员应该都不陌生，这类攻击通常在某些函数提供极大输入或传递非法值时发生。精心设计的安全器件会采用特殊结构来仔细分析每个输入，拒绝所有不可接受的输入。
- **信息泄露：**
  除了预料中的 I/O 通道之外，信息还可以通过其他方式从器件传递到攻击者。工作时序有时可能会显露出一些关于内部机密信息的内容。攻击者可以在一段时间内测量流入器件的电流，观察是否在某种情况下存在异常的大/小电流。有时可能会有某种可以测量的电磁辐射。尽管没有任何器件可以针对各种已知或未知的泄漏提供完美保护，但安全器件设计人员熟悉这些攻击，可以大幅提高保护等级。

结论

考虑到声誉、安全、责任和利润等多方面原因，应该将硬件身份验证纳入全新设计。高质量的身份验证解决方案可保护各种产品免遭克隆、欺诈性修改、机密信息泄露或其他类型的滥用。受保护的元素可能包括软件/固件模块、媒体文件、医疗耗材及记录、电池和打印机碳粉盒等电子消费品以及过滤器和无线或网络传输等用途的其他零售消费品。

如果设备或主机设备包含某种微处理器或主机计算机，则可以使用现代身份验证器件为设计带来前所未有的安全级别。这类器件采用久经验证的加密算法，可简化实现过程，因此设计人员不必是加密专家。

在为产品选择身份验证解决方案时，设计人员需要针对其应用在成本、安全性和速度之间取得适当的平衡。此外，设计人员还应考虑产品在市场上的生命周期，以确保身份验证机制的安全性能够一直持续到产品的使用寿命结束。

对于不需要大量存储空间、设备存储器不同部分不需要不同加密保护以及同一设备上不需要多种算法的应用，加密身份验证 IC 能够以适合大多数大众市场的价格提供最高级别的安全性。

尽管摩尔定律指出，伪造者能够借助计算成本越来越低而计算速度越来越快的发展趋势制造克隆设备或破解密钥，但这也意味着合法 OEM 可以获得成本越来越低而安全性越来越高的高安全性设备。至于密钥长度，自然是越长越好。

版本历史

版本	日期	说明
A	2020 年 5 月	本文档的初始版本。本文档取代 Atmel 文档 8668B（2013 年 7 月）。

Microchip 网站

Microchip 网站（www.microchip.com/）为客户提供在线支持。客户可通过该网站方便地获取文件和信息。我们的网站提供以下内容：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题解答（FAQ）、技术支持请求、在线讨论组以及 Microchip 设计伙伴计划成员名单
- **Microchip 业务**——产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、Microchip 销售办事处、代理商以及工厂代表列表

产品变更通知服务

Microchip 的产品变更通知服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请访问 www.microchip.com/pcn，然后按照注册说明进行操作。

客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（ESE）
- 技术支持

客户应联系其代理商、代表或 ESE 寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过 www.microchip.com/support 获得网上技术支持。

Microchip 器件代码保护功能

请注意以下有关 Microchip 产品代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术规范。
- Microchip 确信：在按照操作规范正常使用的情况下，Microchip 系列产品非常安全。
- Microchip 重视并积极保护其知识产权。任何试图破坏 Microchip 产品代码保护功能的行为均可视为违反了《数字器件千年版权法案（Digital Millennium Copyright Act）》并予以严禁。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。

法律声明

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，将来可能会发生更新。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 https://www.microchip.com/en-us/support/design-help/client-supportservices。

商标

ISBN：978-1-6683-0403-7

质量管理体系

有关 Microchip 的质量管理体系的信息，请访问 www.microchip.com/quality。

全球销售及服务网点

美洲	亚太地区	亚太地区	欧洲
公司总部 2355 West Chandler Blvd. Chandler, AZ 85224-6199 电话：480-792-7200 传真：480-792-7277 技术支持： www.microchip.com/support 网址： www.microchip.com **亚特兰大** 德卢斯，佐治亚州 电话：678-957-9614 传真：678-957-1455 **奥斯汀，德克萨斯州** 电话：512-257-3370 **波士顿** 韦斯特伯鲁，马萨诸塞州 电话：774-760-0087 传真：774-760-0088 **芝加哥** 艾塔斯卡，伊利诺伊州 电话：630-285-0071 传真：630-285-0075 **达拉斯** 阿迪森，德克萨斯州 电话：972-818-7423 传真：972-818-2924 **底特律** 诺维，密歇根州 电话：248-848-4000 **休斯顿，德克萨斯州** 电话：281-894-5983 **印第安纳波利斯** 诺布尔斯维尔，印第安纳州 电话：317-773-8323 传真：317-773-5453 电话：317-536-2380 **洛杉矶** 米慎维荷，加利福尼亚州 电话：949-462-9523 传真：949-462-9608 电话：951-273-7800 **罗利，北卡罗来纳州** 电话：919-844-7510 **纽约，纽约州** 电话：631-435-6000 **圣何塞，加利福尼亚州** 电话：408-735-9110 电话：408-436-4270 **加拿大 - 多伦多** 电话：905-695-1980 传真：905-695-2078	**澳大利亚 - 悉尼** 电话：61-2-9868-6733 **中国 - 北京** 电话：86-10-8569-7000 **中国 - 成都** 电话：86-28-8665-5511 **中国 - 重庆** 电话：86-23-8980-9588 **中国 - 东莞** 电话：86-769-8702-9880 **中国 - 广州** 电话：86-20-8755-8029 **中国 - 杭州** 电话：86-571-8792-8115 **中国 - 香港特别行政区** 电话：852-2943-5100 **中国 - 南京** 电话：86-25-8473-2460 **中国 - 青岛** 电话：86-532-8502-7355 **中国 - 上海** 电话：86-21-3326-8000 **中国 - 沈阳** 电话：86-24-2334-2829 **中国 - 深圳** 电话：86-755-8864-2200 **中国 - 苏州** 电话：86-186-6233-1526 **中国 - 武汉** 电话：86-27-5980-5300 **中国 - 西安** 电话：86-29-8833-7252 **中国 - 厦门** 电话：86-592-2388138 **中国 - 珠海** 电话：86-756-3210040	**印度 - 班加罗尔** 电话：91-80-3090-4444 **印度 - 新德里** 电话：91-11-4160-8631 **印度 - 浦那** 电话：91-20-4121-0141 **日本 - 大阪** 电话：81-6-6152-7160 **日本 - 东京** 电话：81-3-6880-3770 **韩国 - 大邱** 电话：82-53-744-4301 **韩国 - 首尔** 电话：82-2-554-7200 **马来西亚 - 吉隆坡** 电话：60-3-7651-7906 **马来西亚 - 槟榔屿** 电话：60-4-227-8870 **菲律宾 - 马尼拉** 电话：63-2-634-9065 **新加坡** 电话：65-6334-8870 **台湾地区 - 新竹** 电话：886-3-577-8366 **台湾地区 - 高雄** 电话：886-7-213-7830 **台湾地区 - 台北** 电话：886-2-2508-8600 **泰国 - 曼谷** 电话：66-2-694-1351 **越南 - 胡志明市** 电话：84-28-5448-2100	**奥地利 - 韦尔斯** 电话：43-7242-2244-39 传真：43-7242-2244-393 **丹麦 - 哥本哈根** 电话：45-4485-5910 传真：45-4485-2829 **芬兰 - 埃斯波** 电话：358-9-4520-820 **法国 - 巴黎** 电话：33-1-69-53-63-20 传真：33-1-69-30-90-79 **德国 - 加兴** 电话：49-8931-9700 **德国 - 哈恩** 电话：49-2129-3766400 **德国 - 海尔布隆** 电话：49-7131-72400 **德国 - 卡尔斯鲁厄** 电话：49-721-625370 **德国 - 慕尼黑** 电话：49-89-627-144-0 传真：49-89-627-144-44 **德国 - 罗森海姆** 电话：49-8031-354-560 **以色列 - 若那那市** 电话：972-9-744-7705 **意大利 - 米兰** 电话：39-0331-742611 传真：39-0331-466781 **意大利 - 帕多瓦** 电话：39-049-7625286 **荷兰 - 德卢内市** 电话：31-416-690399 传真：31-416-690340 **挪威 - 特隆赫姆** 电话：47-72884388 **波兰 - 华沙** 电话：48-22-3325737 **罗马尼亚 - 布加勒斯特** 电话：40-21-407-87-50 **西班牙 - 马德里** 电话：34-91-708-08-90 传真：34-91-708-08-91 **瑞典 - 哥德堡** 电话：46-31-704-60-40 **瑞典 - 斯德哥尔摩** 电话：46-8-5090-4654 **英国 - 沃金厄姆** 电话：44-118-921-5800 传真：44-118-921-5820