

ATECC608A 和 ATECC508A CryptoAuthentication™ 器件之间的差异

作者: *Karthikeyan Logaswamy*
Microchip Technology Inc.

简介

ATECC608A 是 Microchip CryptoAuthentication™ 系列高安全性加密器件的新成员，它将世界一流的基于硬件的密钥存储与硬件加密加速器相结合，以实现各种身份验证和加密协议。

应用

与 ATECC508A 相比，ATECC608A 提供了额外的功能，可轻松集成到资源受限的系统中、缩短操作时间、并减少主机和器件之间的事务数。新增功能包括用于实现传输层安全 (Transport Layer Security, TLS) (1.1、1.2 和 1.3) 的安全引导和会话密钥。这些功能提供了安全的 IO 保护密钥，以便在主机和器件之间安全传输密钥。

ATECC608A 器件具有灵活的命令集，可在许多应用中使用，其中包括：

- 网络/物联网 (Internet of Things, IoT) 节点端点安全——管理节点身份验证以及会话密钥的创建和管理，并支持包括 TLS 1.2 (及更早版本) 和 TLS 1.3 等多种协议的完整临时会话密钥生成流程。
- 安全引导——通过验证代码摘要并可选择在验证成功时使能通信密钥来支持单片机 (MCU) 主机的安全引导。此外，还提供了多种配置以提升性能。
- 短小报文加密——通过硬件高级加密标准 (Advanced Encryption Standard, AES) 引擎加密和/或解密短小报文或数据，如个人可识别信息 (Personally Identifiable Information, PII)。该器件直接支持 AES-ECB 模式，在主机的帮助下还可支持其他 AES 模式。附加 Galois 域乘法 (Galois Field Multiply, GFM) 计算功能支持高级加密标准/Galois 计数器模式 (AES-GCM)。

- 软件下载的密钥生成——支持为已下载映像生成本地保护密钥。既支持将一个映像广播到多个系统 (每个系统都具有相同的解密密钥)，也支持点对点下载每个系统的独特映像。
- 生态系统控制和防伪——验证系统或组件的真实性。

ATECC608A 与 ATECC508A 器件兼容，但也存在有限的例外情况。只要正确配置 ATECC608A，针对 ATECC508A 编写的软件通常也适用于 ATECC608A。更多信息，请参见 [“ATECC508A 到 ATECC608A 的移植”](#) 一节。本应用笔记列出了 ATECC608A 和 ATECC508A 在特性、命令和配置方面的差异，并对这些差异的细节进行了概括介绍。有关命令和配置的详细信息，请参见 ATECC608A 数据手册。

参考资料

- [ATECC608A 产品详细信息](#)
- [ATECC508A 产品详细信息](#)

特性

以下部分将介绍ATECC608A相对于ATECC508A新增的各种特性、更新的特性以及删除的特性。

新特性

安全引导

ATECC608A提供一种机制来支持联网MCU/MPU（微处理器）中的安全引导操作，这有助于识别主机上是否已安装欺诈代码。上电时，主机MCU内的引导代码会将代码摘要和/或签名发送到ATECC608A。如果签名使用存储在ATECC608A中的公钥验证摘要，或者将摘要与存储的摘要进行比较，则会向MCU主机返回一条报文。它还可以采用不同的方法缩短引导过程的执行时间，从而实现安全的引导速度优化。为了避免中间人（Man-in-the-Middle, MITM）攻击，ATECC608A会将可选的报文验证代码（Message Authentication Code, MAC）值返回给MCU主机进行验证。

密钥派生函数

ATECC608A支持密钥派生函数（Key Derivation Function, KDF），从预主密钥中派生出KDF密钥。最终派生的KDF密钥主要用于TLS事务。ATECC608A支持三个密钥派生函数：伪随机函数（Pseudo Random Function, PRF）、AES和基于HMAC的提取和扩展KDF（HKDF）。PRF用于TLS版本1.2，HKDF计划用于TLS版本1.3。

AES

ATECC608A支持128位硬件AES引擎，可加密和/或解密短小报文或数据包。它支持电子代码块（Electronic Code Block, ECB）模式和适用于AES-GCM的GFM计算。

自检

ATECC608A提供了一种机制来测试内部加密引擎。它支持对称散列算法（Symmetric HASH Algorithm, SHA）、AES、随机数发生器（Random Number Generator, RNG）、椭圆曲线Diffie-Hellman（Elliptic Curve Diffie-Hellman, ECDH）、椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm, ECDSA）验证和ECDSA签名函数的自检。自检既可以在器件上电或唤醒时运行，也可以在主机发出自检命令时运行。

IO保护密钥

针对ECDH、KDF、Verify和Secure Boot命令，ATECC608A提供一种方法来保护此器件与主机MCU之间的IO传输。IO保护密钥是存储在槽中的随机生成的密钥，由主机MCU和器件共享。

例如，从ECDH生成的预主密钥或生成的KDF密钥由IO保护密钥加密。加密后的密钥将发送到主机，主机随后使用IO保护密钥对其进行解密。在安全引导过程和签名验证过程中，将使用IO保护密钥生成MAC，随后将其发送到主机，以此为主机增加一道验证。

持久锁存位

持久锁存位是易失性存储器中的一个位，用于向器件指示已使能关联密钥与加密功能配合使用。只要V_{CC}保持高于2V，它就会保持其状态。它在上电时始终设置为0，可以通过相应操作进行控制。当槽中的密钥链接到持久锁存位时，将根据持久锁存位的状态激活/禁用槽中的密钥。有四种方法可以控制持久锁存位：易失性密钥使用、安全引导、授权输出和入侵检测。当上述方法之一成功运行时，持久锁存位将置1，从而使能指定槽中的密钥。

易失性密钥使用权限

易失性密钥用于控制持久锁存位的状态。易失性密钥必须是MCU和器件之间共享的机密信息。主机和器件之间的加密操作由易失性密钥来完成。如果成功加密，则持久锁存位会置1，从而使能槽中与持久锁存位关联的密钥。

可编程I²C地址

ATECC608A极具灵活，即便配置区域已锁定也可更改I²C地址，但仅限一次。该特性有助于动态更新器件地址，甚至是在器件已部署到现场的情况下。

计数器匹配

计数器匹配功能提供了一种机制来更改第一个单调计数器（计数器0）递增计数的限值。当计数器0达到计数器匹配槽的限值时，可将密钥应用连接到计数器以防止其被使用。槽中的计数器匹配值可以更改任意次。每次更改时，计数器0都会链接到新的限值。

传输/使用锁定

在以加密方式使能器件之前，器件的通用用途将处于禁止状态。加密操作由槽中存储的密钥来完成，已知密钥由主机提供。加密操作成功后，ATECC608A即可正常使用。

降低功耗

ATECC608A提供了降低功耗的选项。但降低功耗的代价是执行时间会变长。当器件用于低功耗应用时，该选项会很有帮助。请参见“[配置区域更新](#)”一节。

改进操作的附加缓冲区

ATECC608A提供了新的SRAM缓冲区：报文摘要缓冲区、备用密钥缓冲区和SHA上下文缓冲区。当TempKey寄存器保存其他信息时，可以使用报文摘要缓冲区和备用密钥缓冲区。此外，该器件还减少了器件和主机之间的事务，并且可以直接从缓冲区执行不同的命令。

ATECC608A支持使用SHA上下文执行SHA计算的多个实例。SHA缓冲区有助于主机对SHA上下文执行读写操作，从而支持主机执行SHA计算的多个实例。

更新特性

TempKey缓冲区大小增加了32个字节，从而可为其他命令（如AES和KDF等）提供更多存储空间并方便操作。

ATECC608A包含增强型高质量加密随机数发生器，该发生器是通过结合非确定性噪声（熵）源（NRBG）和为根据美国国家标准及技术研究所以（National Institute of Standards and Technology, NIST）标准实现的确定性算法（DRBG）提供种子实现的。NRBG用于实例化，并且每次需要RNG编号时也可以使用NRBG。

不支持的特性

ATECC608A删除了EEPROM可一次性编程（One Time Programmable, OTP）消耗模式。当器件配置区域锁定后，不允许对OTP区域进行任何更改，仅允许读取OTP区域数据。

密钥15的有限密钥使用或LastkeyUse功能已删除。ATECC608A槽15的功能与其他槽相同，不能用于有限密钥使用。

使用选择器字节在单线接口（Single-Wire Interface, SWI）模式下操作时，从共用相同介质的多个器件中选择器件的功能已删除。

命令

以下部分将详细介绍ATECC608A新增的各种命令、更新的命令以及删除的命令。

新命令

SECURE BOOT

安全引导命令在引导期间验证用户应用程序代码。该命令支持三种模式：

- 完整模式。签名和摘要传送到ATECC608A。槽中的公钥验证发送的签名和摘要。响应可以是布尔值或MAC，具体取决于安全引导命令。
- 完整存储模式。在完整存储模式下，摘要或签名存储在槽中。如果摘要存储在槽中，则将其发送到器件进行验证。如果签名存储在槽中，将摘要发送到器件，器件随后将使用存储的签名和公钥对摘要进行验证。
- 完整复制模式。当安全引导代码更新用户应用程序时，将运行该模式。摘要和签名均发送到器件，器件随后将使用存储的公钥对摘要和签名进行验证。成功执行命令后，摘要或签名将复制到槽，具体取决于配置区域中的安全引导设置。

在需要线路保护的情况下，该命令可选择通知器件已将加密摘要发送到器件。在这种情况下，使用IO保护密钥和TempKey对摘要进行加密。器件的返回值是基于所选摘要加密的要验证的MAC或状态代码。发送加密摘要时，器件将返回MAC。主机还会使用IO保护密钥、nonce和摘要来计算MAC，并验证返回的MAC。如果是在完全存储签名模式下，则还要使用签名来计算MAC，并且主机将验证返回的MAC。该命令可选择禁止安全引导功能，直到下一次重启电源。

SELF-TEST

自检命令用于测试AES、SHA、ECDH、ECDSA验证、签名和RNG等加密引擎。该命令具有不同的模式，有助于单独测试各个加密引擎，也可以将这些不同的模式组合使用。器件的返回状态会给出各个加密引擎的测试结果。

AES

AES命令支持128位高级加密标准（电子代码簿（AES-ECB）加密和AES-ECB解密），并可计算输入数据的GFM。加密和解密操作一次执行16个字节。

该命令支持选择16字节AES密钥，该密钥可从以下任何来源获取：

- TempKey——从TempKey的16个字节中选择一个作为密钥
- 槽——从槽的16个字节中选择一个作为密钥

器件的返回值是加密/解密数据、GFM数据或错误代码。

KDF

KDF命令用于从预主密钥和输入数据生成KDF密钥。

该命令支持三种创建KDF密钥的模式：

- AES——该模式选择16字节密钥位置的来源
- PRF——该模式选择用于关联数据的认证加密（Authenticated Encryption with Associated Data, AEAD）的源密钥的长度。它还用于选择要生成的目标密钥的长度。
- HKDF——该模式可灵活选择源位置输入数据和零密钥。HKDF中有一个IV特殊函数，用于将输入数据的字符串与配置区域中的预定义字符串进行比较，并在发生匹配后生成KDF密钥。

该命令选择源密钥的源位置，并可以选择目标KDF密钥位置。此附加功能可提高安全性，且无需将KDF密钥返回给器件。源密钥位置和目标密钥位置可以是EEPROM槽、TempKey或备用密钥缓冲区。该命令还提供以纯文本或加密方式将KDF密钥发送到主机的选项。主机使用IO保护密钥和nonce对已加密的KDF密钥进行解密。

根据模式的不同，命令的返回值为纯文本/已加密的KDF密钥或返回状态代码。如果返回已加密的KDF密钥，则还会返回随机的nonce，以便在主机中解密KDF密钥。

更新的命令

ECDH

ECDH 命令还可以选择源私钥位置和目标预主密钥位置。私钥位置的两个可能来源是 **TempKey** 和 **EEPROM** 密钥槽。目标预主密钥位置可以包含以下任何位置：输出缓冲区、**EEPROM** 或 **TempKey**。

当 ECDH 命令选择加密模式时，使用 IO 保护密钥对输出预主密钥进行加密。

GENKEY

GENKEY 命令现在支持针对 **TempKey** 生成新的私钥，生成的私钥仅由 ECDH 命令使用。当私钥存储在 **tempkey** 中时，将释放槽以供其他用途。生成的私钥用于生成预主密钥。

INFO

更新后的 INFO 命令可置 1 和复位持久锁存位的状态。该命令有助于读取持久锁存位的当前状态。

NONCE

Nonce 命令允许将输入数据存储在以下任一缓冲区中：**TempKey** 缓冲区、报文摘要缓冲区或备用密钥缓冲区。在直通模式下，Nonce 命令还允许将最多 64 个字节传送到 **TempKey** 或报文摘要缓冲区。

SHA

SHA 命令支持写入和读取上下文切换，这样便可同时计算多个 SHA 摘要。SHA 模式之前仅支持固定的 64 字节数据，经过更新后可支持可变长度数据。命令的输出指向以下任一位置：输出缓冲区和 **TempKey**、输出缓冲区和报文摘要缓冲区、或仅输出缓冲区。

SIGN

除了对 **TempKey** 中的报文进行签名之外，Sign 命令还提供报文摘要缓冲区中的报文以对数据进行签名，从而释放 **TempKey** 以进行其他操作。

VERIFY

除了对 **TempKey** 中的报文进行验证之外，Verify 命令还提供报文摘要缓冲区中的报文以对数据进行验证，从而释放 **TempKey** 以进行其他操作。该命令具有一个附加模式，可以将 MAC 从器件发送到主机，其中 MAC 是根据 IO 保护密钥计算得出。

不支持的命令

PAUSE

对于 ATECC508A，当 SWI 接口上有多个器件时，Pause 命令很有用。该命令允许 ATECC508A 仅选择与选择器字节匹配的器件执行进一步通信，而与该器件共享同一介质的所有其他器件均进入空闲模式。ATECC608A 中已删除选择器字节功能。

HMAC

尽管 ATECC608A 不再支持 HMAC 命令，但仍可以执行 HMAC 计算。ATECC608A 提供了使用 SHA 命令计算 HMAC 值的功能。在 ATECC608A 和 ATECC508A 中，使用 SHA 命令生成的 HMAC 值始终匹配。但是，使用 ATECC608A 中的 SHA 命令计算得到的 HMAC 值与使用 ATECC508A 中的 HMAC 命令计算得到的 HMAC 值不匹配。

配置区域更新

表1列出了ATECC608A配置区域中新增的位域，并介绍了这两款器件之间的差异。

表1: 配置区域更新

字节	ATECC608A	ATECC508A
13	AES_Enable——该字节用于使能/禁止AES和KDF命令的AES功能。	保留供将来使用
18	CountMatch——该字节用于使能/禁止CountMatch功能并选择用作计数器匹配密钥的槽。	OTP模式——用于为OTP区域设置只读或消耗模式
19	ChipMode——ChipMode字节中的bit 3-7用于定义器件的功耗/时序模式。支持三种可能的模式。可通过更改内部时钟分频比来降低功耗，但代价是执行时间会变长。 Bit 0用于指示在配置区域锁定后是否可更改I ² C地址。 新字节有助于通过其三种模式降低器件的功耗。该字节还可用于选择源I ² C地址，即I ² C_Address或UserExtraAdd字节。	芯片模式
68	UseLock——该新字节用于控制传输锁定功能。它用于使能/禁止传输锁定功能以及用作传输密钥的槽。	LastKeyUse (16字节)——该位域用于控制KeyID 15有限使用功能
69	VolatileKey权限——该新字节用于使能/禁止易失性密钥功能，并为易失性密钥功能选择易失性密钥槽。	
70-71	SecureBoot——该新字节用于配置安全引导功能： <ul style="list-style-type: none"> • 选择其中一种安全引导模式 • 是否在成功执行安全引导命令后将持久锁存位置1 • 用于摘要/签名的槽 • 用于公钥的槽 • 用于安全引导命令的随机数发生器 	
72	kdfIvLoc——KDF (HKDF) 输入字符串内的索引，应包含其下存储的两个字节 (KdfIvStr)	
73	KdfIvStr——KDF (HKDF) 特殊IV模式的KDF报文中必须包含的两个字节的KDF IV字符串	
85	UserExtraAdd——如果非零，则是该器件将在总线上响应的I ² C地址	选择器字节——选择哪个器件将在执行Pause命令后保持工作模式。
90	ChipOptions 新字节具有以下特性： <ul style="list-style-type: none"> • 是否在上电或唤醒时自动运行自检 • 使能/禁止IO保护密钥 • 使能/禁止KDF AES功能 • 设置ECDH和KDF保护功能 • 用于IO保护密钥的槽 	保留供将来使用
96-127	KeyConfig——在KeyType中，增加了两个新类型 (AES和SHA) 以及基于持久锁存位的状态使能密钥的功能。	KeyConfig

ATECC508A到ATECC608A的移植

与ATECC508A相比，ATECC608A支持更多特性。ATECC508A到ATECC608A的移植十分简单，可实现与ATECC608A中相同的特性，但也有一些例外（前面部分已进行了讨论）。要使ATECC608A以类似于

ATECC508A的方式工作，必须按表2所示更改配置区域。请注意，该项配置未使用与ATECC608A关联的新特性或命令。此外，ATECC608A不支持ATECC508A的某些特性（OTP消耗模式、Slot15的LastkeyUse和Pause命令）。

表2: ATECC508A到ATECC608A的移植

字节	ATECC608A	ATECC508A
18	CountMatch——0x00	OTP模式 0xAA——只读模式 0x55——消耗模式 所有其他值均保留
19	ChipMode——字节的bit 3-7应为0	
68	UseLock——0x00	LastKeyUse——通常初始化为0xFF
69	VolatileKey权限——0x00	
70-71	SecureBoot——0x0000	
72	kdfivLoc——0x00	
73	KdfivStr——0x00	
85	UserExtraAdd——0x00	选择器字节——任何值，取决于针对暂停命令配置的器件
90	ChipOptions——0x00	保留供将来使用 0x00

AN2589

注:

请注意以下有关 **Microchip** 器件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指标。
- **Microchip** 确信：在正常使用的情况下，**Microchip** 系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以 **Microchip** 数据手册中规定的操作规范来使用 **Microchip** 产品的。这样做的人极可能侵犯了知识产权。
- **Microchip** 愿与那些注重代码完整性的客户合作。
- **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。任何试图破坏 **Microchip** 代码保护功能的行为均可视为违反了《数字千年版权法案 (Digital Millennium Copyright Act)》。如果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

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。

本出版物中所述的器件应用信息及其他类似内容仅为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。**Microchip** 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。**Microchip** 对因这些信息及使用这些信息而引起的后果不承担任何责任。如果将 **Microchip** 器件用于生命维持和 / 或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切伤害、索赔、诉讼或费用时，会维护和保障 **Microchip** 免于承担法律责任，并加以赔偿。除非另外声明，在 **Microchip** 知识产权保护下，不得暗或以其他方式转让任何许可证。

商标

Microchip 的名称和徽标组合、**Microchip** 徽标、**Adaptec**、**AnyRate**、**AVR**、**AVR** 徽标、**AVR Freaks**、**BesTime**、**BitCloud**、**chipKIT**、**chipKIT** 徽标、**CryptoMemory**、**CryptoRF**、**dsPIC**、**FlashFlex**、**flexPWR**、**HELDO**、**IGLOO**、**JukeBlox**、**KeeLoq**、**Kleer**、**LANCheck**、**LinkMD**、**maXStylus**、**maXTouch**、**MediaLB**、**megaAVR**、**Microsemi**、**Microsemi** 徽标、**MOST**、**MOST** 徽标、**MPLAB**、**OptoLyzer**、**PackTime**、**PIC**、**picoPower**、**PICSTART**、**PIC32** 徽标、**PolarFire**、**Prochip Designer**、**QTouch**、**SAM-BA**、**SenGenuity**、**SpyNIC**、**SST**、**SST** 徽标、**SuperFlash**、**Symmetricom**、**SyncServer**、**Tachyon**、**TempTrackr**、**TimeSource**、**tinyAVR**、**UNI/O**、**Vectron** 及 **XMEGA** 均为 **Microchip Technology Inc.** 在美国和其他国家或地区的注册商标。

APT、**ClockWorks**、**The Embedded Control Solutions Company**、**EtherSynch**、**FlashTec**、**Hyper Speed Control**、**HyperLight Load**、**IntelliMOS**、**Liberio**、**motorBench**、**mTouch**、**Powermite 3**、**PrecisionEdge**、**ProASIC**、**ProASIC Plus**、**ProASIC Plus** 徽标、**Quiet-Wire**、**SmartFusion**、**SyncWorld**、**Temux**、**TimeCesium**、**TimeHub**、**TimePictra**、**TimeProvider**、**Vite**、**WinPath** 和 **ZL** 均为 **Microchip Technology Inc.** 在美国的注册商标。

Adjacent Key Suppression、**AKS**、**Analog-for-the-Digital Age**、**Any Capacitor**、**AnyIn**、**AnyOut**、**BlueSky**、**BodyCom**、**CodeGuard**、**CryptoAuthentication**、**CryptoAutomotive**、**CryptoCompanion**、**CryptoController**、**dsPICDEM**、**dsPICDEM.net**、**Dynamic Average Matching**、**DAM**、**ECAN**、**EtherGREEN**、**In-Circuit Serial Programming**、**ICSP**、**INICnet**、**Inter-Chip Connectivity**、**JitterBlocker**、**KleerNet**、**KleerNet** 徽标、**memBrain**、**Mindi**、**MiWi**、**MPASM**、**MPF**、**MPLAB Certified** 徽标、**MPLIB**、**MPLINK**、**MultiTRAK**、**NetDetach**、**Omniscient Code Generation**、**PICDEM**、**PICDEM.net**、**PICkit**、**PICtail**、**PowerSmart**、**PureSilicon**、**QMatrix**、**REAL ICE**、**Ripple Blocker**、**SAM-ICE**、**Serial Quad I/O**、**SMART-I.S.**、**SQI**、**SuperSwitcher**、**SuperSwitcher II**、**Total Endurance**、**TSHARC**、**USBCheck**、**VariSense**、**ViewSpan**、**WiperLock**、**Wireless DNA** 和 **ZENA** 均为 **Microchip Technology Inc.** 在美国和其他国家或地区的商标。

SQTP 为 **Microchip Technology Inc.** 在美国的服务标记。

Adaptec 徽标、**Frequency on Demand**、**Silicon Storage Technology** 和 **Symmcom** 为 **Microchip Technology Inc.** 在除美国外的国家或地区的注册商标。

GestIC 为 **Microchip Technology Inc.** 的子公司 **Microchip Technology Germany II GmbH & Co. & KG** 在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

© 2019, **Microchip Technology Inc.** 版权所有。

ISBN: 978-1-5224-4831-0

有关 **Microchip** 质量管理体系的更多信息，请访问 www.microchip.com/quality。

全球销售及及服务网点

美洲

公司总部 **Corporate Office**
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 1-480-792-7200
Fax: 1-480-792-7277

技术支持:
<http://www.microchip.com/support>

网址: www.microchip.com

亚特兰大 Atlanta
Duluth, GA

Tel: 1-678-957-9614
Fax: 1-678-957-1455

奥斯汀 Austin, TX
Tel: 1-512-257-3370

波士顿 Boston
Westborough, MA
Tel: 1-774-760-0087
Fax: 1-774-760-0088

芝加哥 Chicago
Itasca, IL
Tel: 1-630-285-0071
Fax: 1-630-285-0075

达拉斯 Dallas
Addison, TX
Tel: 1-972-818-7423
Fax: 1-972-818-2924

底特律 Detroit
Novi, MI
Tel: 1-248-848-4000

休斯敦 Houston, TX
Tel: 1-281-894-5983

印第安纳波利斯 Indianapolis
Noblesville, IN
Tel: 1-317-773-8323
Fax: 1-317-773-5453
Tel: 1-317-536-2380

洛杉矶 Los Angeles
Mission Viejo, CA
Tel: 1-949-462-9523
Fax: 1-949-462-9608
Tel: 1-951-273-7800

罗利 Raleigh, NC
Tel: 1-919-844-7510

纽约 New York, NY
Tel: 1-631-435-6000

圣何塞 San Jose, CA
Tel: 1-408-735-9110
Tel: 1-408-436-4270

加拿大多伦多 Toronto
Tel: 1-905-695-1980
Fax: 1-905-695-2078

亚太地区

中国 - 北京
Tel: 86-10-8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重庆
Tel: 86-23-8980-9588

中国 - 东莞
Tel: 86-769-8702-9880

中国 - 广州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青岛
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 沈阳
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 苏州
Tel: 86-186-6233-1526

中国 - 武汉
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦门
Tel: 86-592-238-8138

中国 - 香港特别行政区
Tel: 852-2943-5100

中国 - 珠海
Tel: 86-756-321-0040

台湾地区 - 高雄
Tel: 886-7-213-7830

台湾地区 - 台北
Tel: 886-2-2508-8600

台湾地区 - 新竹
Tel: 886-3-577-8366

亚太地区

澳大利亚 Australia - Sydney
Tel: 61-2-9868-6733

印度 India - Bangalore
Tel: 91-80-3090-4444

印度 India - New Delhi
Tel: 91-11-4160-8631

印度 India - Pune
Tel: 91-20-4121-0141

日本 Japan - Osaka
Tel: 81-6-6152-7160

日本 Japan - Tokyo
Tel: 81-3-6880-3770

韩国 Korea - Daegu
Tel: 82-53-744-4301

韩国 Korea - Seoul
Tel: 82-2-554-7200

马来西亚 Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

马来西亚 Malaysia - Penang
Tel: 60-4-227-8870

菲律宾 Philippines - Manila
Tel: 63-2-634-9065

新加坡 Singapore
Tel: 65-6334-8870

泰国 Thailand - Bangkok
Tel: 66-2-694-1351

越南 Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

欧洲

奥地利 Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

丹麦 Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

芬兰 Finland - Espoo
Tel: 358-9-4520-820

法国 France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

德国 Germany - Garching
Tel: 49-8931-9700

德国 Germany - Haan
Tel: 49-2129-3766400

德国 Germany - Heilbronn
Tel: 49-7131-72400

德国 Germany - Karlsruhe
Tel: 49-721-625370

德国 Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

德国 Germany - Rosenheim
Tel: 49-8031-354-560

以色列 Israel - Ra'anana
Tel: 972-9-744-7705

意大利 Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

意大利 Italy - Padova
Tel: 39-049-7625286

荷兰 Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

挪威 Norway - Trondheim
Tel: 47-7288-4388

波兰 Poland - Warsaw
Tel: 48-22-3325737

罗马尼亚 Romania - Bucharest
Tel: 40-21-407-87-50

西班牙 Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

瑞典 Sweden - Gothenberg
Tel: 46-31-704-60-40

瑞典 Sweden - Stockholm
Tel: 46-8-5090-4654

英国 UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820