如何使用Microchip安全方案为IoT设备保驾护航（提问精选）

提问人	提问内容	答复内容
etrainchina	目前在IoT应用上，microchip提供了那些解决方案的?	我们为广大客户提供了基于不同云平台的解决方案，从亚马逊AWS，微软的Azure，Ali云服务，并且我们提供标准TLS安全连接的库的支持，方便客户按照自己的要求设计相应的安全解决方案
14778187	如何使用Microchip的LORA模块，以加快物联网设计	microchip Lora模块是支持LORAWAN协议的，
liushiming82	IOT方案主要应用在什么方面呀	目前IoT方案应用在生活的各个方面，包括一些公共设备，如路灯等，井盖，烟感，另外一些生活家电产品，如电子锁，空调等；还有一些工业产品，如厂房里的各种传感器设备。
etrainchina	目前如何保证根节点的安全的?	必須在裝置上存取根節點公鑰以認證該節點之身份
nirvana_xun	IoT的主要安全机制是怎么样的?	IoT的安全包含认证，加密和完整性。 认证可以对称和非对称方式，数据加密通常采用对称AES， 可以通过TLS实现也可以通过自定义的安全协议。 另外，安全的远程升级也是IoT不可少的。

zyh9366	资料可以下载吗?	这次直播的资料会后整理后会发邮件给出席人员
14778	microchip 有哪些代理商?	可以从Mircochip官网查询到
ths9366	应用领域有哪些?	IoT应用领域非常广泛，智能家居，智慧医疗，智慧城市。 可以说无所不在。 有IoT的地方就需要安全， 安全还可以用在代码保护，防配件克隆等。
nirvana_xun	IoT的主要安全机制如何?	主要透過網路層TLS進行雙向身分認證並協議密鑰
ths9366	资料可以下载吗》?	会后将发邮件把相关资料发送给与会人员。
wudianjun2001	物联网外部的话主要是软件来加密吧，要和后台一致。	如果大家都用标准算法，设备就可以与后台一致。Microchip安全产品支持各种国际标准算法。

yedaochang	Microchip IoT 芯片是否已经量产，一级代理商能拿到样片吗?	IoT芯片是指什么？ 安全芯片都已经量产，如果是MCU IoT解决方案，也已经可以从代理商那边获取。
wudianjun2001	MICROCHIP有哪些低成本的加密芯片方案啊?	可使用ATECC608A進行相關算法之運算並安全儲存公私鑰
SUNGUANGZU	IOT可以应用在5G中吗	可以，适用于各种通信协议。
wudianjun2001	Microchip在长三角这边有哪些大的代理?	代理列表可以到Microchip官网查看。 也可以联系本地办公室。
footis	支持哪些加密算法呢	支持SHA256， ECC P256，AES128
bjdavid	是纯硬件加密吗?	是的。

xscc	安全方案支持哪些云服务商	阿里，谷歌，亚马逊云
linux_cc	microchip在IOT上做了哪些安全措施，以保证数据的安全性	不能被解碼
xscc	有评估板提供吗?	MICORCHIP有评估板的
yedaochang	Microchip IoT评估工具包是授权提供使用吗	需要签个简单的NDA
chenlijuan	安全三要素、Hash、对称式和非对称式密码算法 这三者是独立的还是要三者都要包含	安全三要素是加密，认证，完整性。 你提到的几种是不同的算法，看实际的实现，不一定都需要。
yedaochang	IoT 芯片触摸屏控制器接口都是支持电阻、电容屏吧。	安全芯片是协处理器。Micrcochip的AVR和ARM MCU都是支持触摸功能的。

xscc	Microchip的安全器件的低功耗特性如何?	休眠功耗150nA。 执行完后，有定时器自动休眠，下次执行唤醒。
1055875333	Microchip采取什么技术手段进行安全加密?	就加密部分我們推薦使用AES128
liyiui	Microchip IoT 应用方面主打的是安全性么	我們有MCU, 無線通訊模組還有硬體安全芯片
涛声依旧00	加密、解密功耗有多大?	使用Microchip安全芯片在时间上和功耗上比MCU计算有很大优势，具体参数可以查看手册。
btgy4008	硬件加密和软件加密，安全性和易用性综合考虑，采用什么方式好	基本上所有的算法都是公認的,主要的問題在於密鑰的儲放..建議使用硬體芯片處理之
wudianjun2001	软件加密和硬件加密有什么优缺点	硬件加密运行速度会更快，同时可以做安全生态系统，不仅仅是对数据进行加密

htwdb	在加密方式是采用软件算法还是外置加密芯片?	都可以。 但外置加密芯片更安全。 软件算法会有软件漏洞， 密钥在Flash中也很容被读取即使你使能了代码保护。
14778187	如何联系	MICROCHIP在全国10几个城市都有办事处
btgy4008	Microchip支持AES加密吗?	我们的ATECC608A支持AES加密。
wudianjun2001	Microchip有哪些加密芯片，选型表哪里可以下载	我们有多种型号可以选择，包括 ATSHA204A, ATECC508A, ATECC608, 具体可以进下面这个网站了解: http://www.microchip.com/design-centers/security-ics
led2015	代码保护真的可以完全保证吗?	代碼可使用MAC或是用數位簽章確認代碼沒有被竄改
liyiui	Microchip安 带加密引擎的MCU主要有那些型号	基于ARM Cortex 系列有 ATSAML11，ATSAME5X,ATSAME7C

led2015	防止攻击最好的方法，不是法律的严办吗?	：）。 我很赞同。 今天我们讨论技术方案。
qiuhuncl	Microchip安全方案加密芯片支持哪些加密算法	SHA256, ECC P256, AES128
wudianjun2001	一般的无线通讯本身都带加密方面的功能设置吧，方案的加密只能针对用户数据部分吧	不仅仅是对通信的数据进行加密，安全还包括更重要的对身份的验证
dl265361	Microchip加密芯片使用的通讯接口有哪些?	1. High-speed Single Pin Interface, with One GPIO Pin 2. Standard I2C Interface
wudianjun2001	密钥的话是每次通讯都随机改变一次吗?	这个是可以实现的，通过ECDHE来做
wudianjun2001	EEPROM或者FLASH有什么办法保证数据的安全啊?	我们的安全芯片也可以当EEPROM使用，也有专门的加密EEPROM。 有些Flash也自带一些安全机制，有OTP可以写入key。

chenlijuan	目前IoT技术的安全漏洞主要是那些方面	主要有威胁有通信数据被截取，设备被侵入，伪造，克隆等。
zqh1630	microchip的支持RSA算法吗？是硬件产生的?	有支持RSA的，是硬件的。现在主要算法是ECC，它比RSA更安全。RSA需要的密钥长度太长
dwdsp	microchip为安全性提供哪些工具呢?	我们有提供产品的demo，产品的开发资料，库，产品的配置软件，密钥配置工具等。
59477cq	物联网的安全解决方案又那些	算法上有对称，非对称。可以通过软件实现，也可以通过安全芯片。 软件上通过TLS实现安全认证和通信加解密。
18320616	微芯 Microchip 芯片有哪些啊，	ATSHA204, ATECC508, ATECC608
led2015	怎样的设计在理论上才是技术上的完全没有漏洞的安全防范?	基本上現有的算法如MAC ECDSA都是沒有漏洞的算法, 主要的破解都是針對密鑰, 或是使用旁路攻擊 所以必須針對密鑰存放上多用心

zhyouer	对于市面上的第三方IoT云平台的安全性是如何实现?	云平台都有相应的安全机制。 我们的安全芯片来实现这些安全机制。
liyiui	Microchip IoT 怎么做到软更件安全结合在一起了	透過Security Boot來進行對更新軟件的保護..主要技術是使用ECDSA SIGN 和VERIFY
mafeng	加密后数据实时性，会有多大影响?	使用硬件加密引擎，速度很快，如ECDSA的Sign只需要293ms
chenlijuan	ATSAML11 是PIC 32位MCU么	ATSAML11 is Industry’ s first Arm® Cortex®-M23 with robust chip-level security features and Arm® TrustZone® for Armv8-M®
mzlr	采用那些技术应对攻击?	采用先进的安全算法， 密钥使用安全芯片存储，跟人隔离，跟软件隔离，跟生产隔离。同时企业内部管理好安全流程。
led2015	数字签名和密钥，有哪些破解途径?	基本上現有的算法都是沒有安全漏洞的 主要的破解手段都是針對密鑰 透過旁路攻擊是最新的做法

lxl666	IoT 设备可能会有哪些安全问题?	被仿冒访问，被截取数据，被仿冒固件升级，
yyhhgg	；另外里面的序列号可以改变不	序列号是唯一固定的
tlf_2008	加密是否集成在芯片,还是需要适应秘钥配合?	ATECC608A加密在芯片中，密钥在芯片中。
dwwzl	加密方法符合sha么?	符合SHA算法， ECC508/608 带有HMAC选项的SHA-256哈希算法
goyhuan	是不是要HCS300一样的机制?	不是，HCS300是跳码技术。安全芯片包括SHA,ECC,AES，随机数等
nirvana_xun	如果MCU的密级不够，即便安全芯片的层级很高，安全性够吗?	安全关键是密钥，安全芯片可以让密钥跟MCU隔离，软件隔离，所以跟MCU的密级无关。

qiuhuncl	ATSHA204A接口支持哪些协议？速率能达到多少?	支持I2C和单总线。 最大速率支持1M的I2C.
yang_alex	安全芯片和MCU的通讯会不会被监听，从而导致安全性降低?	ATECC608通訊介面可以加密
7905	请简要讲一下，咱这里讲的加密主要指的是对用户程序的防克隆加密还是对应用程序运行时通讯内容保护的加密；如果是防克隆加密的话，那加密机制是在什么时间段：运行时还是偶尔或者启动阶段？独立于主CPU的专有芯片?	您说的Microchip安全产品都可以提供，并且有协议库能够简化开发过程。防克隆一般是在启动阶段做验证，运行时段也可以偶尔做一些校验，但意义不大。今天介绍的产品都是安全协处理器，不是MCU。
led2015	目前世界上最好的计算机针对密码破解，据说位数越多越难破解，是不是真的，目前世界上的最好技术都无法破解的是多少位密码?	以SHA256來說 目前256位元的密鑰就是難以破解的了
btgy4008	认证芯片可以和所有的MCU配套使用吗?	可以的，安全芯片是I2C接口的
wudianjun2001	硬件加密的运行时间大概在什么范围?	你指哪个命令. ATECC608A 的AES128 16字节大概1ms。 非对称的验证和签名大概50ms。

Milo.Bai	可以加密保护flash与ram吗?	安全不是对FLASH和RAM里的数据进行加密，而是对整个产品和系统提供安全保护，包括身份认证，数据加密
yang_alex	目前Microchip有没有集成了安全芯片的mcu?	有不少。 Microchip M0+.M4,M7都有安全引擎的MCU.
飞扬自我	随机发生器最高可以发生多少位的随机码?	32 random bytes
tlf_2008	支持AES硬件，以及DES软件库吗?	ECC608可以支持AES
wudianjun2001	专门加密的EEPROM加密的密钥是固定的吗？还是随机的?	可以在使用之前写入密钥。
zyh9366	接口有哪些?	I2C SWI

footis	硬件加密速率多高	基本上硬體的處理速度在處理各種算法都會在50ms內完成
cruelfox	MCU和外部安全芯片之间I2C通信是很容易被逻辑分析仪抓取分析的，这样会被攻击吗?	部分产品中I2C是加密的。但通常的应用场景，密钥是不会在I2C上传输的，所以不会有安全的隐患。
15986	microchip有汽车电子水泵方案吗	有。 今天主要介绍安全方案， 电机控制方案可以联系我们本地办公室或代理商。
led2015	硬件加密的保护，是否可以做到完全无法破解?	如果破解的难度和代价足够大，就可以认为是安全的。
yang_alex	MICROCHIP方案中云端的安全性怎么保证?	基本上雲端鑰透過ECDSA VERIFY進行裝置連雲的確認
1521837	microchip单片机的thermal pad需要接地吗	是的

yyhhgg	用什么工具把序列号读出来，作为产品的唯一序列号，编程器吗	I2C或SWI接口就可以读出来。
qiuhuncl	相同的封装，如果合理的配置，芯片ATECC508A与芯片ATSHA204A功能上兼容替代么?	ATECC508A 可以覆盖ATSHA204A的功能。
zhyouer	如果云平台将智能设备接入公网就增加了安全风险，如何有效管控呢?	云平台和设备间要相互进行身份认证
hxm3000	以前IOT没见过microchip使用	目前microchip提供在IOT中主芯片,無線連網模組和安全芯片
xscc	提供软件开发的SDK吗?	有CryptoAuthLib
yang_alex	感觉安全芯片就像现在银行手机或PC端的U-Key'? 但和云端怎么同步啊?	对。 先要有一个签发过程，签发是通过私钥签发的， 云端会有对应的公钥验证。

wuxianshuchuan	支持无线吗	安全芯片器主要处理与加密相关的功能，可以适用于有线或者无线的连接。
wojiaomt	密钥得有一套完善的管理体系吧	透過microchip硬體安全芯片可以安全的儲放密鑰並搭配硬體運算 如ATECC608A
linghz	有哪些加密方式?	SHA256 AES128 ECC P256
北方	这个安全协处理芯片是否可以适用在非Microchip的产品，对应安全芯片是否占用周期，是否对运行速度有影响，有多大影响。	可以。 Microchip和非Microchip使用是一样的， 我们提供标准C的库，也提供Linux下的库。
hello_mcu	MICROCHIP的安全机制会使IOT数据传输量变大或者通信更繁琐吗	通信前会有身份认证和密钥协商，会使数据量有所增加，
ths9366	功耗如何?	超低功耗

yedaochang	只是支持Microchip iot平台吗，兼容其它竞争对手 iot平台吗?	可以
tlf_2008	请问密钥可以配几个?	Upto 16
yang_alex	安全协处理器中安全存储是明码存储还是加密后存储？相同内容存储后的内容相同吗?	内部的存储也是加密的。
wudianjun2001	介绍的这些加密芯片，官方都有对应的开发板吗?	Yes.
chenlijuan	嵌入式安全中软件安全 程序算法是不是重要些	Key storage is most important
hxm3000	这个芯片的加密需要单片机编程吗？还是个纯粹的EEROM	是具有加密存储和加解密算法的芯片，需要配合一个主控使用。

yyhhgg	内部时钟如果损坏后，是不是整个芯片就报废了呢	以ATECC608A來說 若是芯片報廢的話密鑰也是不會外流
chenlijuan	Microchip M0+ 上的安全引擎会不会占用比较多的资源 拖慢速度	M0+的安全引擎大部分功能是硬件实现的，所以只占用非常少的资源。
appleliu88	请问方案成熟了吗？是否已经量产？	是的!已量產!!
ths9366	有哪些接口？	I2C和单线接口
zhyouer	对于数据存储不安全如何来避免？	使用具有硬件级加密保存的安全芯片就可以
xscc	IOT设备安全方案的成本如何？	成本问题请联系Microchip本地办公室或代理商。

dcexpert	支持哪些开发工具?	Atmel Studio, IAR, Keil, others
yyhhgg	如果把产品的序列号作为产品唯一的序列号来用，但是如果芯片损坏，需要更换芯片，这样序列号也会跟着变化，上位机软件也会变化，就会给用户带来麻烦，如果可以修改里面的序列号，就不会存在这种情况	開後門的同時就是增加了被攻擊的機會
Laspide	CAN-FD安全性产品有哪些可供选择?	Not release not, please wait
elleny	IoT中采用硬件加密认证比软件加密有哪些优势和好处?	1. 软件加密算法由软件实现，会占用Flash、RAM和处理器资源，而且速度比较慢 2. 软件加密密钥通常放在MCU的Flash中，而Flash内容非常容易被破解读出，所以密钥容易暴露。硬件加密芯片采用特殊的硬件加密半导体工艺，密钥无法读取。 3. 采用硬件加密密钥的预置和分发更容易实现。
xscc	有无线连接方面的安全芯片吗?	建議使用硬體安全芯片 如ATECC608A接在無線模塊上即可
yang_alex	安全协处理器需要编程吗？还是只是当作一个外设？外加MCU来对他操作。	可以通过I2C或SWI接口编程。可以理解成是一个专门负责安全功能的协处理器。

htwdb	Microchip 安全在加密方式采用AES吗？是否支持国密SM?	目前不支持国密。
轻舞	如何用MICROCHIP公司的安全类产品保护IOT节点设备的安全?	从安全性所要考虑的3方面（机密性，完整性，身份验证）对节点设备进行保护：在节点通讯或者数据传输应用中，安全类产品可以提供一种安全保障，以保护与安全相关的信息的机密性以及完整性，在身份验证方面，节点远程升级时能对代码进行鉴定，使系统能在安全的环境下运行；在做数据连接或存储时，对通讯对方进行身份鉴定
goyhuan	芯片有中文资料吗?	SHA204和ECC508有
btgy4008	如果使用mcu实现解密算法，配合烧写软件，通过mcu的ID号进行加密，这种方式与外接加密芯片的方式相比有什么不足（安全性）？	安全不仅仅是对数据进行加密，还包括身份认证，数据完整性等，这样才可以实现系统的安全性
qiuhuncl	针对ATSHA204A OTP模式被锁存, 通过哪些方式可以重新开启OTP模式呢?	锁定以后无法更改。
bigbat	目前支持的非对称算法有哪些？最低配置产品是什么型号?	ECDSA 可使用 ATECC608A

ths9366	算法是什么?	SHA256,ECC,AES等
火星狮子座	加密方法有哪些?	SHA256 AES128 ECC P256
yang_alex	安全协处理器采用哪种标准加密算法？还是说MICROCHIP自己开发的加密算法?	NIST SHA256; ECC P256;AES128;全部是标准的算法。
liyiui	Microchip IoT 是不是要结合Microchip的软硬件才有用了	MCU可以兼容使用其他厂家的
14778187	microchip的FOC方案弱磁怎么计算	今天主要讨论安全解决方案。 电机相关问题请联系Microchip本地办公室或代理商。
led2015	密钥也需要定期修改吗，还是每次使用时都会随机产生?	建議不須修改 在標準算法中 每次驗證都會搭配隨機亂數運算之

nirvana_xun	为什么是72位的序列号	72位序列号是足够长的
led2015	芯片安全设计是否主要靠程序代码?	主要是靠算法和密鑰 故密鑰存放相當重要
18320	如何烧录microchip的贴片式芯片	是的
bkn1860	硬件加密的器件有那些型号	ATSHA204A ATECC508/608
lingf	采用的是硬件加密吗?	是的
gmphoenix	是主控级的方案还是外挂式的方案?	外接的

wudianjun2001	家居内部的无线加密不太重要吧，主要是外部通讯的加密，内部很少有人带设备到家里来进行破解	看具体的产品应用。如果是对家里的灯和电源设备进行控制，不加密就可以被门外的设备控制了。
stclq	开发环境是什么样的?	根据选择的主处理器选择开发环境。 我们有MPLAB IDE 和 Atmel studio作为开发环境。
轻舞	为什么随机数发生器对于一个安全系统来说非常重要?	在一个安全系统中会大量使用到随机数发生器，从安全密钥的产生，到质询响应过程中的随即质询都与此随机数发生器有关。
btgy4008	有了芯片级的安全，是否不用再考虑链路的安全了?	链路层安全也需要考虑的，包括使用密钥协商等方式
rinfen	我们现在的车联网项目对安全要求特别高，特别是涉及安全方面的	是的。 我们已经有汽车级的安全解决方案。
lixiang	Microchip公司对于IoT的应用提供了哪些安全的解决方案?	裝置連雲認證 資料加密 和 資料正確之確認

szyouer	当设备连接到互联网时如何防范数据窃取和欺诈的风险?	连接时使用证书来进行身份认证
liyiui	Microchip IoT 安全方案会不会增加工作量和复杂性	这是肯定的。 我们的方案就是让用户用尽量少的工作量和安全知识来实现高的安全解决方案。
yang_alex	非对称算法中，主机端会知道安全协处理器中的私钥吗?	不會
lingf	批量生产时的密钥维护方便吗?	microchip提供標準的後端生產裝置維護用戶的密鑰
btgy4008	硬件加密回出现加密芯片受干扰损坏而使整个系统瘫痪吗?	不会，只影响该节点
etrainchina	目前可以存储多少对密钥?	Upto 16

飞扬自我	非对称性的身份验证有哪些优势?	优势是双方可以使用不同的密钥，公钥和私钥，且不能由公钥去推算私钥，避免密钥暴露的风险。
yin_wu_qing	是用什么工具烧录程序的？是用到什么接口烧录的?	硬體安全芯片的對外連接口只有I2C 和SWI
SUNGUANGZU	咱们的MCU有样板吗	都可以到microchip网站搜索到相对应的样板
lingf	密钥的写入复杂吗？每个设备都需写入不同的密钥吗?	可以是一樣的，也可以用SN來派生出不同的
dwwzl	万一密钥丢失或者找不到了，怎么办呢?	所以建議將密鑰存放在安全芯片中 若是不見了 也不會洩密
liyiui	安全序列号是自动生成的么？是唯一的么	是安全芯片自带的，出厂时已固定

led2015	每次数据传输，是否都会密钥认证?	密钥是通过一定机制协商的，根据需要进行密钥协商。
btgy4008	只能在Microchip的MCU上用，还是可以支持其他的MCU?	不受限制。但是如果使用Microchip MCU开发工作量就小很多。
tlf_2008	增加安全认证芯片会增加多少成本?	目前安全芯片牌價0.5USD
stclq	提供相关的程序库供用户自行调用吗?	有提供，安全加密软件库，crypto lib,提供源代码
yedaochang	IoT外接NFC 模块，Microchip都配套提供吧。	我们目前没有NFC方案。
wudianjun2001	如果使用随机密钥的EEPROM，EEPROM在使用过程中坏掉的话，板子是不是就要报废了，单独换个EEPROM没用了	不是隨機的，大多是用SN來派生出來的

90houyidai	如果无法连接到签名者，如何使用呢	只要有签名者的公钥就可以验证签名者签发的设备。
wudianjun2001	硬件加密芯片的算法是固定的吧，那密钥是如何产生的	硬件產生私鑰 公鑰可讀出
wojiaomt	从长远考虑，密钥硬体如果升级了，基于旧硬体的密钥是否能延续?	如果是同一系列产品的升级，新产品会有对老产品的兼容。
yedaochang	Microchip 现在有推出AI智能家居与IOT解决应用方案吗	microchip提供主芯片 無限模塊 和安全芯片
wudianjun2001	硬件加密芯片大概什么价格，官方有现成的历程吗?	都有例程
zyh9366	维护方便吗?	硬體芯片配置後不需維護

dl265361	microchip加密芯片在使用中若出现损坏，如何解密之前的数据?	安全芯片不是对数据进行加密保存，主要是身份认证，传输数据加密
1787585	microchip ide 怎么关联编译器xc8	通常XC8安装好会自动关联，在tools菜单的Option下面可以手动关联。
lixiang	使用安全芯片Eccx08A进行TLS连接的相关身份验证及密码交换的好处有哪些?	节省主控MCU实现 TLS的Flash/RAM占用 比纯软件处理更快更省电 使TLS不存在任何密钥泄漏的风险 在生产过程中不需要往主控MCU中烧入任何密钥和证书(这些都是保存在ECCx08A中)
btgy4008	已有的软件中添加CIA是否比较复杂?	使用外加安全协處理器是最簡單的
led2015	密钥写入的过程中是否会被窃取?	非对称式密钥是由安全芯片内部自己产生，私钥是不会泄露出来的
btgy4008	认证芯片可以和所有的MCU配套使用吗?	可以的，

yedaochang	IoT 授权认证要用单独芯片控制吗?	可用單芯片運行OPENSSL
dcexpert	ATMEL Studio还会继续更新吗》还是会合并到 MPLAB IDE X?	以后会逐渐合并到MPLAB x，现阶段还继续支持。
mm88	性价比怎么样	超高性價比
lanlz	用户需要做哪些工作以便将安全功能集成到IOT设备中?	所做的工作是比较多的。Microchip提供了CryptoAuthLib库，兼容多种主流的协议，如WolfSSL,OpenSSL,大大简化开发工作。
shenlan1986	如何保护固件程序	如果是固件防克隆，那可以使用外置安全芯片。
led2015	看出厂设置的配置过程中使用了很多的密钥和证书，是否越多重密钥越安全所以才设置了这么多?	其實單一認證只需要1個斯鑰和一個簽章 使用多少要視功能決定

dcexpert	除了IDE，debug硬件工具以后是否也会统一?	会。
wudianjun2001	MPLAB是不是不提供支持了，都搞到X里面了	已经不升级。建议使用X
wudianjun2001	这个TLS加密是纯软件的吧?	TLS協議是MCU處理的，只有用到ECDH和ECDSA算法的時候用ECCx08來完成
wudianjun2001	这个TLS加密是纯软件的吧?	TLS的AES加解密也可以用ECC608來做
7905	谢谢!刚刚讲到私钥连原厂都没法读解，那有否预防万一连主人都忘了密码的后悔补救措施呢？不至于万一真是忘了就报废吧?	非对称式密钥的公钥和私钥都保存在安全芯片里的，公钥可以读取到，私钥不能被读取。不需要记住密钥的
wyh2013	密钥的加密方式是变化的还是统一的	TLS立面的加密方式是變動的

nirvana_xun	如果兼顾设备的安全性和快速响应	使用Microchip的安全协处理器就可以即提供安全又不影响系统的响应速度，非对称的算法都在毫秒级别完成。
dl265361	批量使用时烧入密钥的工具用哪种?	希尔特的编程器会支持ATSHA204A，Microchip官网有Softlog支持。Microchip工厂支持密钥烧入服务。
14778	microchip单片机大家都是用的什么系列	microchip有ARM與自設計系列
chenlijuan	非对称式身份验证跟其它方式有什么优点了	非对称式身份验证，不会有密钥配送问题，私钥不可以公开，只有自己知道，公钥可以任意公开
hxm3000	这个芯片的开发是否配套主控芯片一起开发？还是可以用一个单独的环境开发这个单芯片?	有ACES單獨配安全芯片
zhimagod	有没有集成加密芯片的单片机或处理器?	有, 例如 ATSAML11.

chenlijuan	Microchip IoT 安全方案怎么帮助没有用过的人尽快上手了	我们有安全开发工具及对应的上位机ACES可以方便上手，也提供完整的库。
xscc	安全芯片支持空中升级 (OTA) 功能吗?	安全芯片内不需要升级固件的。如果您讲的是对MCU的安全升级，安全芯片是有该方案的。
wudianjun2001	这些加密芯片主要有哪些的应用场合啊?	1.配件認證 2.智財保護 3.Security boot 4.密鑰存放 5.IOT
liyiui	非对称式密钥的公钥和私钥 这两个是相互独立的么	这是两个算法相关的密钥，所以不是独立的。
qiuhuncl	真正的密钥只有一个，事先烧入了ATSH204A中，如果项目中的mcu采用AVR单片机，是不是唯一的密钥还要作为KEY烧入单片机的flash rom中参与计算出MAC值来，如此一来，如果要被人破解的话，读出了单片机中的密钥也就知道了ATSH204A中的密钥，何来的安全认证呢?	SHA204是对称式的安全认证，MCU中会存储有KEY，这个是对称式认证的特点。MCU被破解后，只是HEX被泄露，要分析读懂代码才能得到KEY值。这个难度会增加很多。
yedaochang	Microchip IoT 控制芯片都支持七大通信协议吧	支持I2C接口和单线接口方式

dwdsp	加密芯片留有后门么?	当然没有
chenlijuan	Microchip IoT 安全方案可以与云端同步么	可以的
zhimagod	单片机和加密芯片之间的通讯会不会泄露密钥之类的关键信息	不会，通信时不会传递密钥
zhimagod	单片机和加密芯片之间的通讯会不会泄露密钥之类的关键信息	通常密钥不会在通讯总线上出现，单片机和加密芯片的通讯也可以有密钥保护。
mzlr	加密芯片是否支持固件升级?	加密芯片本身不升级，可以实现你的系统的安全的固件升级。
yedaochang	目前Microchip 测试插件/脚本/数据都是开源吗?	microchip提供函式庫源碼給客戶

wudianjun2001	TLS只能对 用户数据进行加密吧，对包头包尾什么的能一起加密吗?	加頭加尾的加密沒有必要 也會讓資料無法傳遞
yang_alex	在进行加密数据通信的情况下，加解密过程对于数据传输速率的影响有多大?	在进行加密数据传输时，一般使用AES加密方式，AES的运算速度很快，对传输速率影响很小
btgy4008	目前IOT标准比较多，领域也很广，如何保证其安全稳定的运行?	建議參考microchip方案進行
qiuhuncl	银行的网盾是不是也是类似的加密方式?	是的， 也是证书认证。现在网盾大都采用RSA
etrainchina	目前支持多大的存储量?	ATECCx08能达到8.5Kb，ATSHA204A是4.5Kb。
mzlr	Microchip 安全方案通过哪些安全认证?	亂數產生器有經過FIPS認證

bobde163	这样的加密的方案，在Lora这样的网络中能适用吗?	可以的
zyh9366	售后服务有哪些点?	除了完整方案的支持降低开发难度，我们还有密钥的配置服务。
chenlijuan	Microchip IoT 芯片主要型号有那些，有什么优点了	SAMG55 WINC1500 ATECC608A 讓使用者容易使用上手
ths9366	售后服务有哪些点?	有技术执线 800 - 820 - 6247 (座机) 400 - 820 - 6247 (手机) 技术支持邮箱: china.techhelp@microchip.com 在公司网站上可以找到您当地所对应的办事处和指定代理商
btgy4008	安全认证器件为MCU/FPGA 提供最安全的保护是不是在外围通过硬件电路连接保护的?	不是。硬件电路只是通过I2C或单总线。 安全的保护是通过安全芯片本身的特性保证的。
chenlijuan	Microchip IoT 中无线协议支持那些了，主流的都支持么	是的。LoRa，蓝牙，WiFi都支持。

zyh9366	数据安全性怎么样?	可以透過SHA256確認數據完整性 用AES128進行加解密
1871824	microchip xc16收费吗	也有免费版的，可以供评估。
yedaochang	支持所有应用接口传感器数据采集吧	可以的 傳感器資料蒐集之後可以透過硬件加密做傳輸
ths9366	维护方便吗?	硬體安全芯偏一經配置之後即不須維護
mzlr	Microchip 安全方案有哪些安全措施?	跨多层的主动屏蔽 内部所有存储器存储内容加密 随机的数学运算 内部状态一致性检查 电压干扰，隔离电源轨 内部时钟发生 安全测试模式，无JTAG 无调试探测点，无测试焊盘
zhyouer	居民家中、工作场所及公共空间里的物联网设备生成的潜在敏感型数据，会在公共互联网中来回穿梭，如何来确保这些数据的安全?	首先需要认证，需要身份识别。另外数据本身要有完整性机制，最后数据本身通过目前被公认有效的算法加密。保护好密钥。

zwjiang	硬件加密支持哪些算法，加解密的时间是多少?	现在有支持SHA256,ECC256,AES等算法，SHA256和AES运算起来很快，ECC的签名和验证是毫秒级的
bkn1860	几种机密芯片的成本如何	請聯繫本地代理商
zyh9366	算法是什么?	我们现在有支持SHA256,AES128, ECC256,后续会有更多的算法支持。
lospring	单片机和加密芯片之间的通讯会不会泄露关键信息，要如何 预防	MCU和安全芯片之间的通信是不进行密钥传输的，
xiwujie	加密有那些方式？什么方式较好。	SHA256 AES128 ECCP256
rinfen	今天的演讲文档可下载吧？贵司是否有相关的白皮书之类的文档可下载?	可以联系今天演讲者邮箱

wudianjun2001	介绍的几种算法哪种在普通MCU上实现比较容易点啊	SHA和AES的对称算法比较容易点，非对称占用的资源多，时间长。
nirvana_xun	TLS在应用上层，怎么保证底层安全?	因為有加入資料簽章 所以若是在底層被攻擊資料傳到上層就會被發覺
7905	所谓的密钥协商是需要MCU在程序运行中主动握手动作的一段程序?	MCU通过调用CryptoAuthLib接口与加密芯片交互，完成这一个过程。
xiwujie	采用MICROCHIP 加密算法安全等级符合那个标准	RNG符合FIPS認證
yedaochang	Microchip 独有 ECDSA(椭圆曲线数字签名算法)签名与验证 官网有开源吗	目前沒有
1871824	microchip xc8 编译器免费了吗	XC8可以免费下载和使用，与完整版的区别是编译效率低一些。

rinfen	非对称加密安全性好，但速度比较慢，在比如汽车数据上传数据量较大时就比较麻烦，请问贵司产品在这方面有比较好的方法吗?	非对称式算法主要用于身份认证，完成身份认证后进行数据传输时，一般还是会采用AES来对数据进行加密
qiuhuncl	对于加密计算方式，Microchip安全方案加密芯片遵循哪些标准?	RNG已經FIPS認證
douglas816	加密安全性会被攻破吗?	一般是攻不破的，或者说攻破需要的代价和时间是不能承受的。
footis	包含通信时间的话，MCU侧加解密速率最高能达到多少	完成身份认证后进行数据传输通信时，一般会采用AES方式进行加密，AES的加解密速度很快
etrainchina	目前有没有一对一沟通的渠道啊?	有的，可以到公司官方网站找到您当地联系方式，或者技术热线：800 - 820 - 6247 (座机) 400 - 820 - 6247 (手机)
rinfen	今天说到的安全模块的代码区和数据区是否和其它部分是隔离的?	这个跟MCU有关。 你可以把安全模块相关代码区打包成库， 带Trust Zone的单片机也支持安全代码的隔离。

qditz	microchip的安全方案可以模块部署?	可用硬體安全芯片加入主系統以增加安全性
wudianjun2001	MPLAB是不是不同的MCU要安装不同的编译器的	主要有8bit，16bit，32bit三种编译器
7905	难道会有不用一点软件配合的纯硬件加密吗?	所謂的硬件加密芯片指的是儲存密鑰和用硬體模組處理算法
7905	难道会有不用一点软件配合的纯硬件加密吗？如没有，那如何界定的软件或者硬件加密呢?	我們提供的硬件加密指的是不耗費軟體資源進行運算算法 並且提供存放密鑰
rinfen	有机会的话，看能否到我们公司交流一下，我们对安全很关注^_^我们非联网设备也有用贵司的产品	請聯繫我們代理商 我們很樂意
guizhou112115	能在Microchip的MCU上用	Microchip 有很多MCU芯片可以配合应用

zhyouer	如何解决服务端存在的用户安全校验简单、设备识别码规律可循、设备间授权不严等安全问题?	安全需要通信的双方按照一定的协议完成。另外服务器端也可使用安全芯片，做到硬件级加密安全。
etrainchina	目前有计划支持5G这块吗?	我們的安全芯片可以加到任何系統中提供主芯片安全支援
1521972	microchip官网买的芯片用什么快递,FEDex还是DHL呢	一般是EMS
xiwujie	针对BLE的控制器IS187, 有没有相关加密	microchip安全芯片可以容易的加到您的系統中透過主芯片通訊提供安全支援
mymyhope	如何保证供应链的安全性?	通过证书的签发过程控制供应链的安全，也可以把密钥烧入过程与供应链无关，比如让第三方或Microchip来实现密钥烧入。
zhyouer	如何确保所有清单内的应用数据在传输过程中得到保护?	采用ECDHE进行密钥协商，可以做到每次通信时都使用不同的密钥

7905	主CPU与安全芯片间握手信号最少要几根物理连线？包括2根电源线?	单总线。 最少2根，支持数据线供电。
wudianjun2001	今天讲的内容会发送到邮箱吗	会的，
btgy4008	在车载或者工业方面都可以适用吗?	是的。
footis	采用IIC接口或者单总线接口与MCU交互的话， 加解密速度会不会比较低?	不會的!! 主要的加解密都是用芯片内部的硬件完成
btgy4008	你们的芯片提供样品吗?	客户可以申请样品的
yedaochang	目前量产Microchip IoT 控制芯片支持多大闪存?	SAMD21 支援256K SAMG55 支援512K

7905	信号协议时序会是专有的吧？用示波器可以破解观察吗？	单总线协议是专有的，可以观察。但是密钥不会在总线上传输。
yedaochang	目前Microchip 芯片PIC系列型号控制很省电，目前主推IoT控制芯片是否传承省电功能。	會
nirvana_xun	安全在上层，会不会不利于安全，能不能防护针对安全的漏洞	因為通訊中有加入簽章 所以若是資料在底層有被破壞則上層會發現並拒絕接收
liangtom125	价格呢？最便宜的mcu几块钱，你们大概价格？	价格问题可联系本地Microchip办公室或代理商。
lark100	入侵检测是类似自检的功能吗？	入侵检测主要是做身份认证，确认访问者身份是否是合法的
www369	8位MCU和508搭配使用时，对8位MCU有那些硬性要求！内存？时钟？等	只要該8位MCU能夠存取I2C 搭配10K內存即可

www369	8位MCU和508搭配使用时，对8位MCU有那些硬性要求！内存？时钟？等	大部分8bit PIC和AVR的都支持，对资源要求很小。
wudianjun2001	官网可以免费申请样品吗?	可以。
led2015	黑客后门主要是什么思路?	主要是讓黑客能夠在必要時候控制該端點對目標進行DDOS攻擊
SUNGUANGZU	: 官网可以免费申请样品吗	可以的
SUNGUANGZU	资料会发邮件吗?	会的
lospring	安全方案都有哪些？与其它公司的产品有什么不同	microchip提供SHA256 ECC508 ECC608 細節請找代理商詳談

ths9366	数据安全性怎么样?	除了认证和完整性，可以对数据进行加密。
zyh9366	安全机制是什么、?	通过认证，完整性和加密还实现。算法上可以使用对称或非对称算法。
www369	有开发教程吗？貌似508要比204难很多吗?	主要是508比204多支援了非對稱的演算法
www369	有开发教程吗？貌似508要比204难很多吗?	我们提供了一系列的例程
dl265361	IOT应用的安全性上有哪些难点需解决?	需要解决和云的相互身份认证
szyouer	如何防止攻击利用Linux系统的漏洞?	所有的漏洞都是為了獲取密鑰 解決軟體問題(如heart bleeding)可以將密鑰存放在microchip硬體安全芯片中 不會外漏

ths9366	安全机制是什么?	通过认证，完整性和加密实现。算法上可以使用对称或非对称算法。
dwwzl	加密狗失效了能否复制?	本身的里机的密钥无法复制，不过可以让Root重新生成一个
gmphoenix	握手时间多久？受什么影响?	握手时间跟算法执行的速度，总线传输速度有关。
yang_alex	使用microchip的安全协处理器芯片，MCU端必须具有硬件加密引擎吗?	不需要，
yang_alex	使用microchip的安全协处理器芯片，MCU端必须具有硬件加密引擎吗?	AES128用软件来做也是很简单的
zhyouer	对于防范移动设备用户面临的设备丢失或被盗造成的风险?	可在雲端後台管理設備的登入 若已經遺失刪除其權限

wudianjun2001	编译器好多家做的吧，哪家的比较常用	GCC, IAR, Keil， etc
wudianjun2001	SAMG55的板卡还是挺不错的，功能很强大，玩过一段时间给网友了，想搞一块收藏。	可以到官网购买 https://www.microchipdirect.com/product/search/all/ATSAMG55-XPRO
btgy4008	保证联网的嵌入式设备的安全，防止非法访问和数据篡改，这些都是棘手的问题。microchip在物联网设备保驾护航方面有何部署?	需要从CIA三个方面去考虑，如果有需求可以联系我们的技术支持
baxk	目前如何进行每个根节点的配置?	节点的话，最重要的是它的密钥对，这个在生产过程中是芯片产生的，但需要对这个密钥对中的公钥进行签名，然后把签名档信息烧录到芯片中
qiuhuncl	针对未授权的解密，设计上Microchip ATSHA204A芯片有哪些物理的安全特性去保护EEPROM内容?	跨多层的主动屏蔽，安全测试模式，无JTAG，无调试探测点，无测试焊盘
wudianjun2001	AS7.0是不是不能装到XP系统的	最新是升级系统，XP确实太老了吧

azhiking	Microchip有没有提供全套的iot解决方案啊?	主芯片 SAMG55 無線模塊 WINC1500 安全芯片 ATECC608A
led2015	目前现有的云端服务有哪些安全隐患?	会受没有认证设备的攻击。
李欢欢	时钟损坏了，怎么维修?	外部时钟坏了，程序可以切换到内部时钟。
qiuhuncl	Microchip安全方案芯片能实现授权密钥的加密方式么?	microchip的安全芯片可以实现授权应用的设计
zhyouer	如果在设计时并没有实现让移动端和服务端支持一套共同的安全需求，有什么方法来实现其安全性?	您指的是密码套件吗？如果是密码套件，这个是需要双方沟通协商好的，如果不同的话，是无法进行安全连接的
btgy4008	嵌入式物联网如何处理安全策略?	连接的认证，数据的完整性和安全性。采用安全的远程升级。

machinnneee	我们的安全芯片和市场 同行有什么优势?	我们有丰富的安全经验。 芯片安全等级高，性价比高。
machinnneee	我们的安全芯片和市场 同行有什么优势?	我们在安全领域耕耘多年，对于安全我们有更深刻的认识，比如我们的主动安全屏蔽是覆盖全区域的，还有我们的防旁路攻击的手段也更全面
led2015	多级硬件安全保护在设计中是否还有什么漏洞?	这个是没有什么漏洞的，但关键是密钥的存储