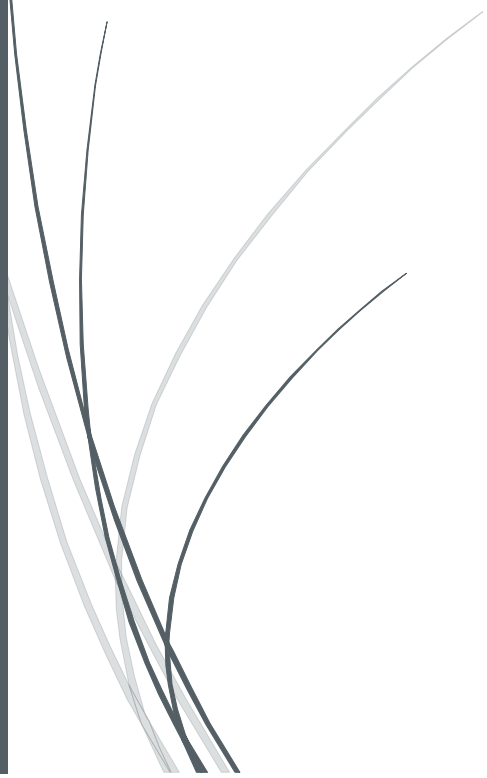
INPLAY INC

7/25/2019

一种基于低功耗蓝牙 SoC 的低成本的加密鉴权认证方法技术白皮书



INPLAY INC

摘要

随着基于低功耗蓝牙技术的消费类及物联网产品的蓬勃发展，开发者和系统管理员对产品及系统的安全性越来越关注。基于蓝牙技术的产品及系统的安全性，真实可靠及安全不仅关乎产品品牌的信誉，同时也对企业营收及运营带来潜在风险！本文提出对无线物联网产品及系统加密鉴权的技术，并通过应用实例阐述此技术可能带来的商业价值及未来可以承载服务的新的机制。

内容目录

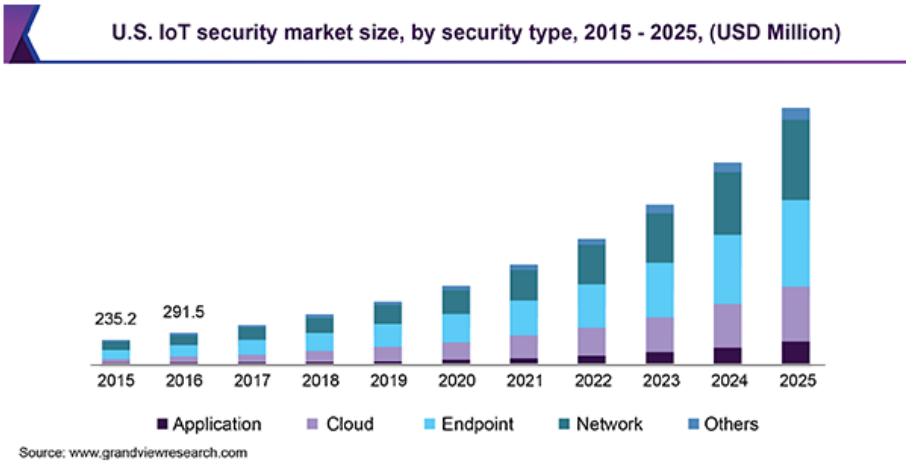
图表

表格

产业背景

全球物联网 (IoT) 安全技术市场规模在 2017 年的时候为 12.4 亿美元。在预测期内, 其复合年增长率可能上升到 29.7%。物联网是最重要的技术趋势之一, 吸引了全球多家公司的关注。随着物联网产品在无线网络、人工智能和机器学习领域的日益整合, 加上传感器和微控制器的开发, 市场对产品的安全性需求也逐渐浮出水面。

互联 IoT 技术的日益使用使得组织网络和设备越来越容易受到安全漏洞的攻击, 层出不穷的安全漏洞事件越来越引起消费者和企业对网络攻击的认识。具有网络和计算功能的智能设备正在医院、家庭、城市和制造业里广泛部署，这些新兴的互联设备及网络大大提高了能源效率, 增强了患者管理, 并优化了制造工艺。尽管好处很多, 但这些系统中的安全漏洞正在引起用户的不满。因此, 解决物联网领域的安全挑战预计将在预测期内推动市场增长。图表 1 是美国一家研究机构给出的安全技术市场规模和营业预测，可以看出市场对安全物联网节点的需求正以前所未有的速度增长。



图表 1 美国 IoT 设备安全市场状况及预期

无线物联网因为其便捷灵活的部署方式及低成本，越来越多的系统使用者选择无线物联网解决方案。然而，无线物联网设备及网络产品应为其无线属性，任何人都可以方便的监听其网络上流动的信息（尤其在 ISM 公共无线频段内工作的设备），这为无线产品及网络带来了更多的潜在隐患。

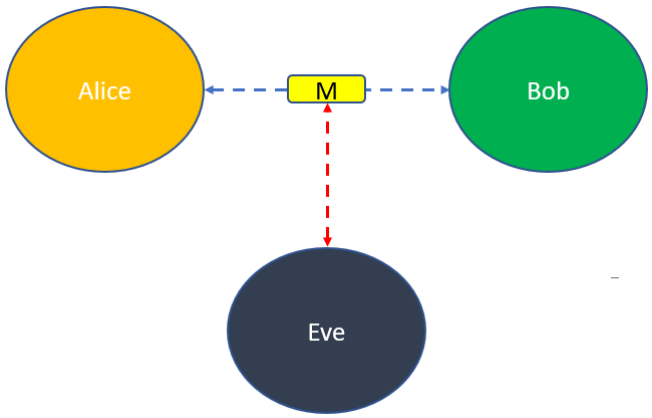
安全加密技术的几个概念

数据的有效性和完整性

在无线通讯领域里，数据的完整和有效是非常重要的一个要求。如图表 2 所示，Alice 如果发送信息 M 给到 Bob，当 Bob 收到 M 的时候，数据 M 的完整性保证了其在无线传输过程中没有被 Eve 所篡改。

一般来讲，Hash 技术因为其不可逆推演而被用来解决数据不可篡改，其可以把任意长队的输入通过散列运算变换成固定长度的输出，其输出即为 Hash 值。任何一个输入文件数据位的变化都会导致 Hash 运算的结果产生翻天覆地的变化，这为校验数据文件是否被修改提供了非常便利的数学运算工具。目前比较流行的算法有 MD5, Hash-1 和 Hash-2 等, 区别是数学运算难度，Hash-2 因为比特数多因而反推演难度更大，其在安全应用中比较流行。在嵌入式应用中，比较热门的 MCU 安全校验启动功能即采用 Hash 运算功能以确保设备在确认软件没有被他人篡改后才会正常启动，否则系统将放弃启动。这一属性特点对物联网应用及其重要。

虽然解决了数据 M 的完整性的问题，但是 Bob 收到的 M 是否真的是 Alice 发送的呢？如图表 2 所示，如果 Eve 在通讯链路上伪装成 Alice 并告诉 Bob 自己发送的 M 是真实的信息 M，Bob 如何分辨呢? 这就引入了第二个概念-数据来源的真实性。

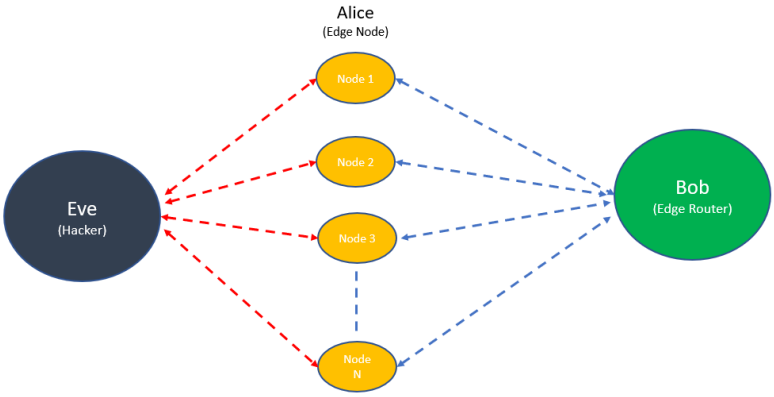


图表 2 安全漏洞拓扑模型

数据来源的真实性

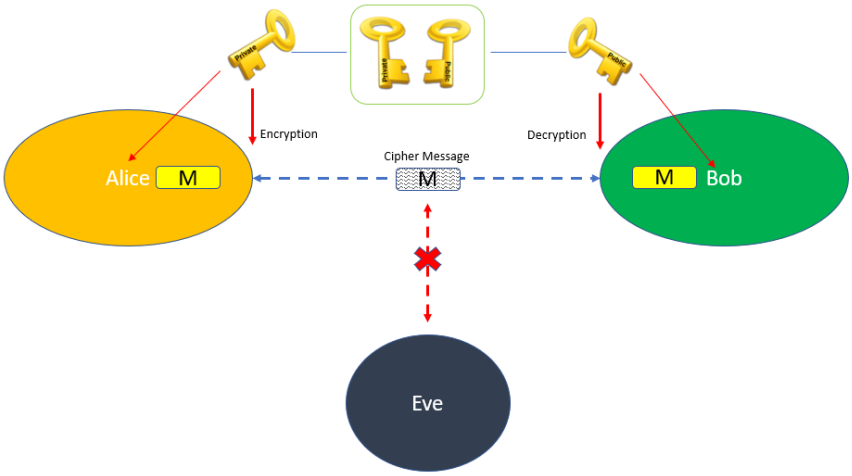
当 Alice 发信息 M 给到 Bob 的时候，Bob 需要确保 Alice 作为发送信息的人的真伪，这就需要一种技术来实现对发送数据的来源做验真操作，又称为鉴权。这种技术今天在互联网非常通用，类似于 Https 中的”s”, 代表安全认证操作。同理，在无线物联网领域，类似的技术也不断涌现，有同密认证系统，也有非对称认证系统。

同密认证系统在 Alice 和 Bob 侧采用同样的密钥，这将确保 Bob 在收到信息 M 的时候用同样的密钥认证确认消息是否从 Alice 发出，只有拥有同样密钥的人才能打开消息 M。当今广泛采用的同密加密技术有 AES-128, AES-192 和 AES-256。这种系统应用简单明了，但是对于网络较大的应用则不是很合适，因为此种方式需要全网络分享统一的密钥，一旦任意节点密钥被泄露，全网络将全部受到安全威胁，如图表 3 所示，Eve 有机会破坏任意一个节点并获取其存有的密钥，一旦成功获取，Eve 将获得整个网路的控制权。而且同密系统导致密钥分发环节很不容易把控，在节点端分发密钥的做法让密钥分发管理很难操作执行。



图表 3 同密系统被干扰模型

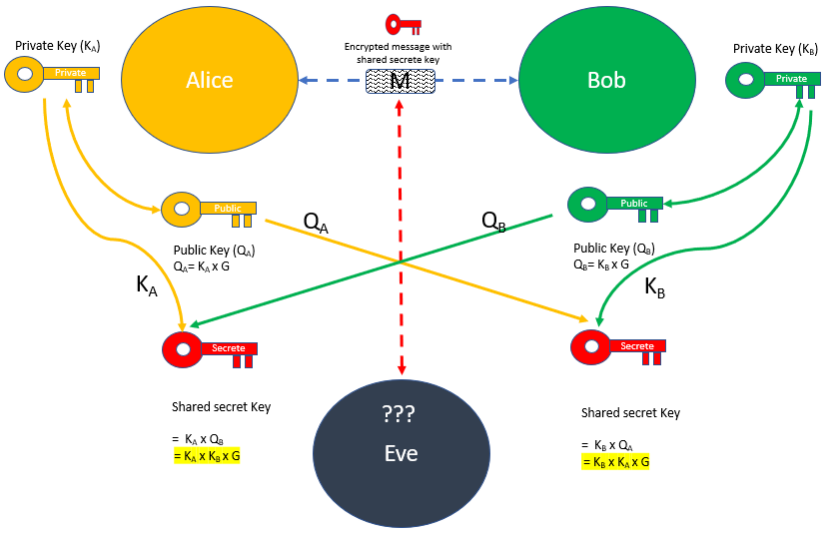
非对称认证系统采用公有密钥和私有密钥配对方式，此类系统又被称为公钥密码学系统。此种系统需要的是一组单方向很容易计算但是逆推很难的算法。非对称加密认证是目前市场上最为流行的安全加密技术，因为它不需要密钥离开设备，只是通过交换信息和做数学运算即可认证对方的真伪，这极大降低了网络管理的难度，同时从根本上解决了密钥分发的难题。以图表 4 为例，Alice 与 Bob 建立联系前需要认证对方的真伪，Alice 和 Bob 通过非对称加密方式产生一对公有/私有密钥对，Bob 拥有公有密钥，Alice 拥有私有密钥。Alice 在发送信息 M 前先通过私有密钥对信息进行加密，Bob 收到信息 M 后用公有密钥对其解密，如果运算正确，则 Bob 确认此信息 M 来自于 Alice，因为共有/私有密钥对的特殊数学运算关系，只有拥有公有密钥的人才可以确认信息 M 的真实来源。Eve 因为没有私有密钥，所以无法加密信息 M 并伪装成 Alice。此逻辑和同密系统类似，但是不同的是非对称加密系统可以解决网络系统多节点认证鉴权问题，多个网络节点可以拥有同样的公有密钥，而局端设备拥有一个私有密钥即可，节点和局端设备通讯可以确保局端设备的真实可靠性。反之，如果局端设备需要认证节点设备的真实可靠性，节点端则需要拥有私有密钥，而在局端设备需要拥有公有密钥。目前市场上比较流行的非对称加密算法有 RSA 和 ECC（椭圆曲线算法），ECC 因为其占用系统资源少，运算速度快从而越来越受系统开发者青睐并正在快速成为网络隐私与安全保护的首选解决方案。



图表 4 非对称认证系统模型

数据消息的保密性

节点和局端设备的认证鉴权做好后，通讯数据本身的保密性则是由对数据加密实现的。通常比较流行的对称加密算法有 AES-128，AES-192 或 AES-256，数据位数越大，加解密难度越大。这往往可以确保无线数据不是以明文方式发送，而是通过密文发送的，从而使得任何网路监听者都无法获取信息的明文数据。对称加密本身的算法是容易理解的，但是，对称加密用的密钥如何产生呢？如果采用同密系统，密钥分发又变成了不易解决的一个问题。所以，目前流行的密钥分发系统多采用非对称算法生成共享密钥。而非对称算法中 ECC （椭圆曲线算法）又最为流行。采用 ECC 算法生成一对公有/私有密钥，这一生成密钥对的协议算法称之为 ECDH。ECDH 协议定义密钥对如何生成并在 Alice 和 Bob 之间如何交换，如图表 5 所示，Alice 和 Bob 希望采用对称加密的方式建立连接并交换信息，第三方 Eve 可以获取空中信息，但是无法解码通讯信息 M。



图表 5 非对称加密共享密钥生成

首先，Alice 和 Bob 各自产生他们自己分别的公有/私有密钥对，Alice 有私钥 K_A 和公钥 $Q_A = K_A \times G$, Bob 有私钥 K_B 和公钥 $Q_B = K_B \times G$，这里 Alice 和 Bob 需使用同一参数 G 作为椭圆曲线算法的参数项。

然后，Alice 和 Bob 在公开渠道交换其拥有的公钥，Eve 此时可以获取双方的公钥，但是因为 Eve 没有 Alice 和 Bob 的私钥，由于 ECC 算法的不可逆性，他也无法通过反向推演椭圆曲线算法解出私钥，因此 Eve 无法算出共享密钥。

Alice 在拿到 Bob 的公钥后计算共享密钥 $Key = K_A \times （K_B \times G）$, 同理，Bob 也通过 Alice 的公钥计算他的共享密钥 $Key = K_B \times （K_A \times G）$。这里你可以容易的发现双方获得了同一个密钥值。这就是 ECDH 算法共享密钥的生成过程。

有了共享密钥，Alice 和 Bob 就可以通过对称加密的方式进行通讯而无需担心被第三方窃听或破译的问题。

值得一提的是，ECDH 因为其不需要通讯双方预先设定密钥，这为动态共享密钥生成提供了一个很好很安全的解决方案。一旦 ECDH 密钥生成协议被采用，通讯双方只需动态建立非对称密钥对以实时生成所需的对称加密密钥。这对没有 I/O 及显示的无线物联网产品设备及其有用，设备与主机之间建立连接的时候可以采用 ECDH 算法而无需通过人为的输入手段生成加密密钥以保证通讯的安全可靠。这可以大大简化系统硬件的设计及降低系统成本。

表格 1 总结了上述谈到的三种安全加密技术的概念和特性。

表格 1 安全加密算法特性总结

	数据完整性	数据来源真实性	数据保密性
HASH 算法	是	否	否

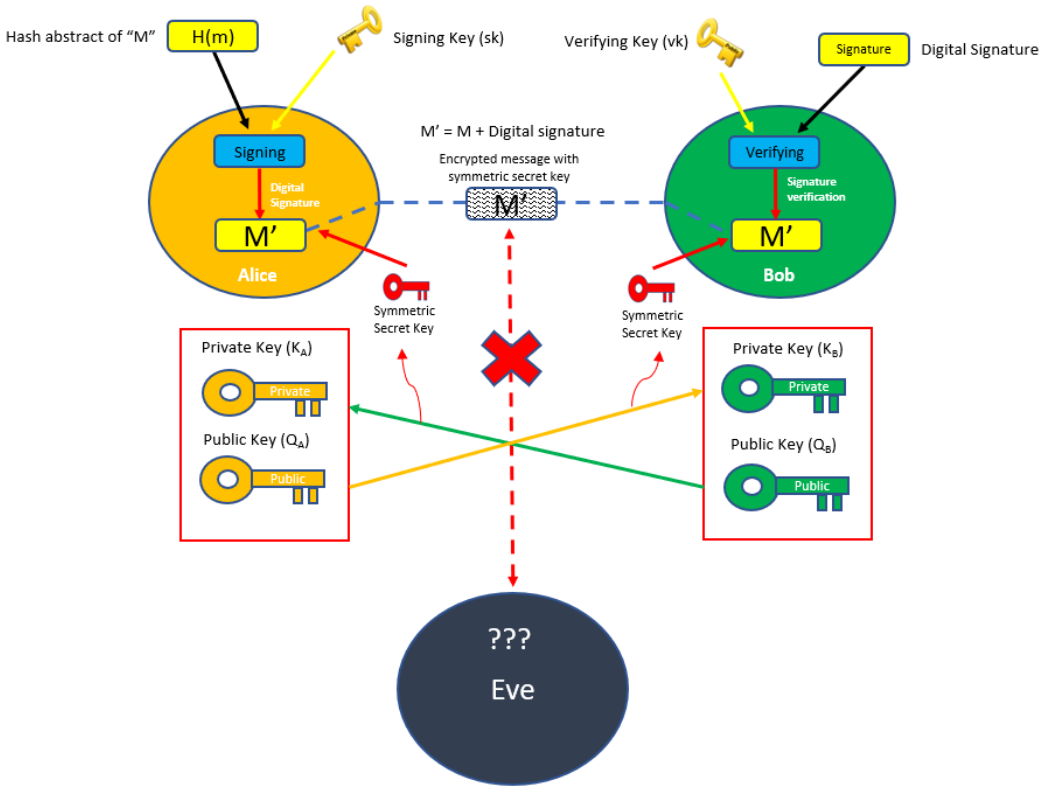
数字签名算法	是	是	否
数字签名加密算法	是	是	是

采用 ECDSA 数字签名技术的加密算法协议

前述提到安全加密技术的几种概念并对数据完整性，真实性及保密性分别做了概念阐述。在无线物联网应用中，如何采用最简单有效的方式把三种需求融合起来统一解决呢？接下里我们介绍的方案即可以满足三种需求的全面要求，为物联网开发者提供了一种全新的安全加密解决方案。

图表 6 简单示意了如何利用基于 ECDSA 数字签名技术并结合 ECDH 做共享私钥动态生成算法以满足前述的几种需求。首先，Alice 把要发送的消息 M 做 hash 运算产生一个固定位数的哈希值，这便于签名算法的快速简单计算，同时 Hash 运算也保证了信息 M 的完整性和一致性。Alice 用自己的认证私钥作为 Signing Key (sk)对此哈希值做 ECC 椭圆曲线数学运算，并生成数字签名，此数字签名会连同信息 M 一并作为待发送的信息，此处用 M'表示。接下来，Alice 和 Bob 之间要通过 ECDH 密钥交换协议产生共享密钥，此共享密钥即为同密密钥，并被作为 Alice 和 Bob 之间交换信息的密文编解码密码。Bob 在收到信息 M'后对其解密并生成原始信息 M 和它的数字签名，然后用 Bob 存有的认证公钥作为 Verifying Key (vk)对数字签名做验证运算，因为只有和认证私钥配对的公钥才可以顺利完成计算，如果计算结果通过，则表明此消息 M 确实为 Alice 发送过来，从而完成对信息发送者的验真工作。

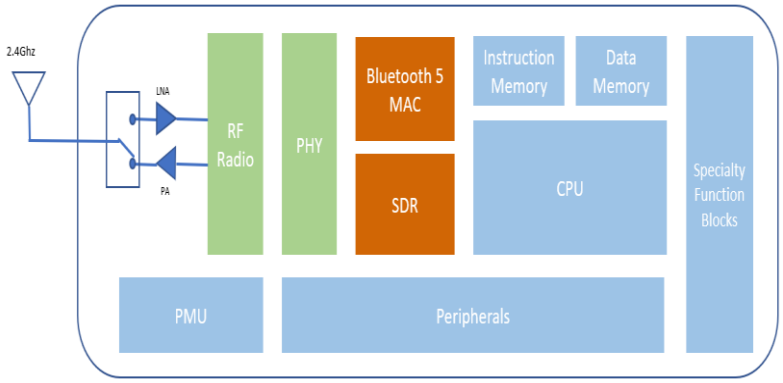
通过 ECDSA 的签名算法和 ECDH 的共享密钥生成算法，信息完整性，信息来源的真实性及保密性全面得到保障，这种安全加密机制从根本上解决了开发者对安全加密的设计挑战，并提供了可供实施的整体解决方案。



图表 6 采用 ECDSA 数字签名的加密算法协议

介绍 InPlay SwiftRadio™ SoC

InPlay SwiftRadio™ SoC 是一款基于 2.4GHz 射频工作频段的无线 SoC。图表 7 示意了 SwiftRadio™ SoC 芯片的系统框图。它集成了超低功耗 2.4GHz 射频收发器，调制解调器，InPlay 私有多模协同通讯协议（其中包含蓝牙 5 和 InPlay 软件定义无线电（SDR/2.4GHz 私有协议））和片上电源管理单元；此芯片还集成了主频高达 64Mhz 的带浮点运算处理单元的高性能 Arm Cortex-M4F 微处理器及子系统，包含 256KB ROM，1MB Flash Memory 和高达 96KB 的用户 SRAM。SwiftRadio™ SoC 集成了独立的硬件安全引擎给开发者编程安全应用，例如 AES256, SHA256 和 ECC256。同时芯片内部集成了私有 ECDSA 数字签名算法协议及基于 ECDH 协议的共享密钥生成算法协议，方便用户开发符合未来市场安全需求的无线物联网产品及系统。为保证密钥的不可篡改，芯片集成了专用的 OTP（一次性可编程）存储器以方便用户存储公钥。同时，芯片支持认证授权安全启动，从而确保产品的固件是被认证的正确的和没有被篡改过的固件。

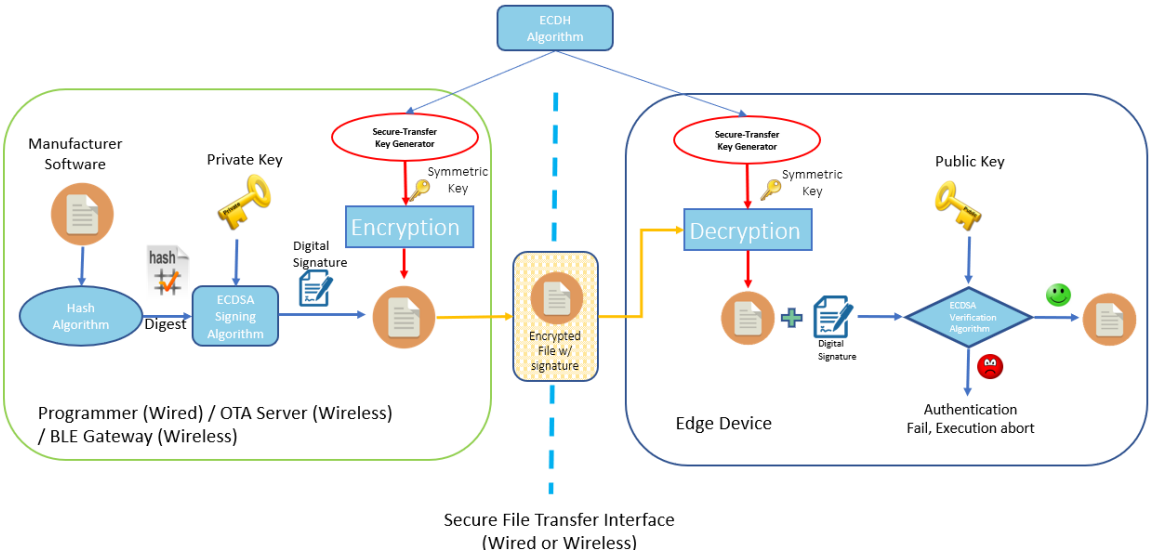


图表 7 InPlay SwiftRadioTM SoC 系统框图

InPlay 私有 ECDSA 数字签名加解密算法协议

为了满足无线物联网市场日益增加的对数据安全加密及认证的需求，InPlay 成功开发了私有 ECDSA 数字签名算法协议及基于 ECDH 协议的共享密钥生成算法，可以充分满足开发者对信息来源认证，信息完整性及保密性的全部诉求。

图表 8 展示了烧录器/OTA 服务器/蓝牙网关等（以下简称“主机”）与终端设备（以下简称“从机”）之间的基于 InPlay 私有加密鉴权协议的流程图。本文仅以主机对从机发送更新软件的应用为例解释加密鉴权协议的工作流程。同样的流程可以应用于对数据传输的安全保护和设备鉴权验真应用。首先，当主机和从机需要建立连接事件前，主机需要先将文件做 Hash 运算并产生一个固定位数的哈希值，然后主机用存在于主机内部的私有密钥对其进行 ECC 签名算法运算并生成一个数字签名。同时主机和从机各自通过 ECDH 算法协议动态生成各自的非对称公钥/私钥对，并交换彼此产生的公钥给到对方，然后主机和从机用自身存储的非对称私钥和收到的对方公钥进行 ECC 对数运算并生成共享加密密钥，此密钥即被主机作为明文文件的加密密钥。最后，主机将经过加密的密文文件和数字签名一并发给从机。从机收到后首先对数字签名进行鉴权认证，它将预先存储于从机设备内的公钥取出与收到的数字签名文件同时作为 ECDSA 签名验证算法的输入条件并进行验证运算，如果结果为“真”，则证明收到的加密文件确实为主机所发送过来的，否则从机设备将拒绝此文件接收。鉴权确认完成后，从机将用通过 ECDH 协议算法生成的共享密钥作为解码密码并对收到的密文进行解码最终得到明文文件，这样主机和从机就完成了一次文件加密传输即鉴权的操作。



图表 8 InPlay 私有数据文件加密鉴权传输协议

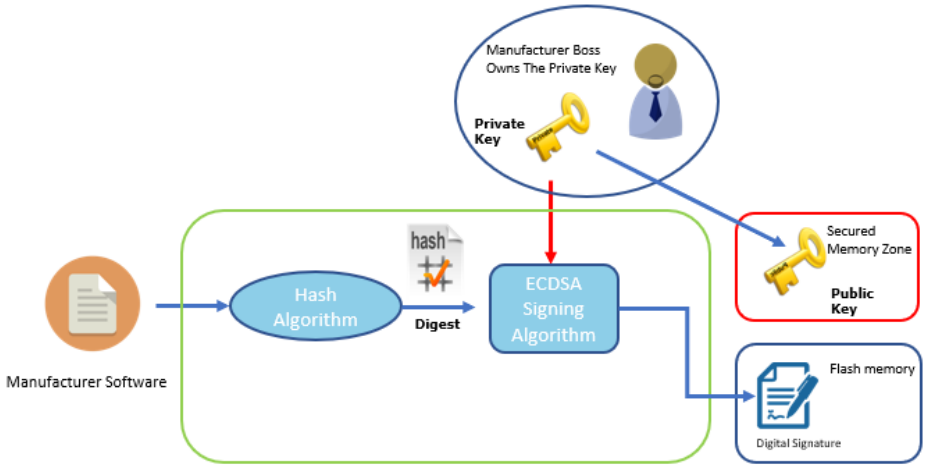
如下代码示例给出了一个非常简单的通过鉴权加密做数据通讯的从机例程。开发者只需增加几行非常简单的代码即可实现安全的无线通讯应用设计。

```
// read public key from efuse0
pub_key = efuse_read_word(EFUSE0_ID);

// ecdsa verification
pka_init();
if (rom_ecdsa_verify(1, pub_key,buffer, auth_hash))  {
    DBG("Auth verify failed\r\n");
    return -1;
}

// gen public key
gen_pub_key(1, priv_key, pub_key);

// gen aes key
gen_shared_secret_key(1, priv_key, buffer,secret_x);
hash_start(2, &ctx);
hash_preprocess(2, &ctx, secret_x, 32);
hash_finish(2, &ctx, aes_key);

//send public key
send(pub_key);
```

图表 9 和图表 10 和示意了另外一种如何利用 InPlay 私有 ECDSA 数字签名鉴权协议做安全程序启动的应用实例。

在产品和系统设计或生产过程中，为了确保用户应用程序的来源是真实可靠的，开发者可以利用 Hash 算法和 ECDSA 算法对程序文件做数字签名生成，如图表 9 所示。开发者需要通过 ECC 算法生成一对非对称的公钥/私钥对并需要严格保护好私钥，一旦泄露私钥，此安全程序启动功能即面临安全威胁，程序

文件鉴权即存在风险。在工厂应用程序烧录的时候，生成的公钥需要被存储/烧录在芯片的 OTP（仅可编程烧录一次且不可修改的）存储器区域，而生成的数字签名可以被存储在 Flash 存储器中。

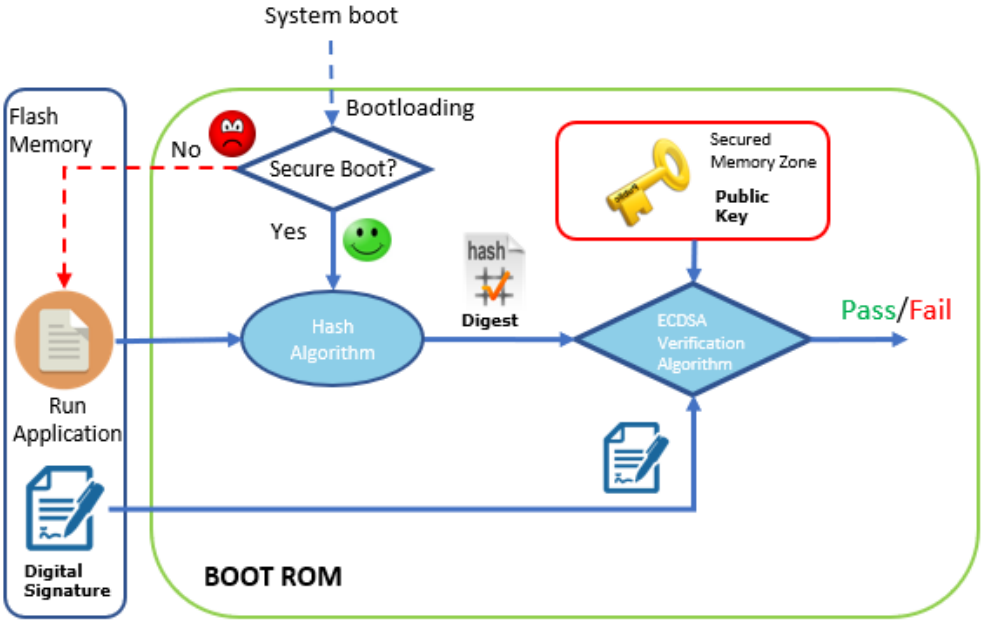


图表 9 安全程序启动鉴权数字签名生成

开发者可将如下几行代码加入烧录器程序中，即可简单实现应用程序数字签名生成设计。

```
1.  //calculate hash
2.  sha256_init(&sha_ctx);
3.  sha256_update(&sha_ctx, data, data_bytes);
4.  sha256_final(&sha_ctx, hash);
5.
6.  /// Signed it
7.  const struct uECC_Curve_t *curve = uECC_secp256r1();
8.  uECC_sign(m_priv_key, hash, 32,m_signaure,curve);
```

在产品开机启动后，系统的启动程序开始运行并检查安全启动选项是否有被使能？（使能开关设置是开发者在生产产品时预烧录好的并不可更改），如果没有使能，系统指针直接跳转到正常应用程序运行的起始地址。一旦确认安全选项被使能，则内置到芯片 BOOTROM 里的启动程序将对程序文件做 Hash 运算生成哈希值，并将预存在 Flash 存储器中的数字签名和预存在不可修改存储器中的公钥一并作为输入参数送入 ECDSA 算法做数字签名验证运算，如果结果通过，则证明程序文件来源真实并未经篡改，从而进入正常应用程序运行模式，否则，程序将停止执行。这种带数字签名鉴权的安全启动特性从根本上解决了开发者担心的上市产品软件被任意篡改或来源不明的危险。



图表 10 安全启动程序鉴权签名验证

如下代码示例给出了一个通过鉴权数字证书验证做安全启动的例程。

```
// calculate hash
hash_calc(hash, pbr);

// ecdsa verification
pka_init();
if (ecdsa_verify(1, pub_key,secure_signature, hash))  {
    DBG("ecdsa verify failed");
    return -1;
}
```

总结

InPlay 公司提出了一种在蓝牙 SoC 上直接集成创新的安全加密算法及协议，采用国际上推崇的 ECDSA 数字证书加密技术及基于 ECDH 协议的密钥生成技术，从而大大降低了开发者开发安全的无线物联网产品及系统的成本并加快了上市时间。基于此技术的应用将确保开发者专注于应用层面的价值开发，而无需担心其产品及系统在市场上潜在的安全威胁。

关于 InPlay

上海橙群微电子有限公司（“InPlay”）是一家无晶圆半导体芯片设计公司, 总部位于中国上海并在美国加州设有分公司。团队成员曾为美国著名的半导体公司工作，该团队的主要专长是无线和移动通信系统领域, 在射频、模拟混合信号电路和低功耗电路设计方面拥有独特的技术。公司专注开发无线物联网单芯片系统 (SoC) 及解决方案, 致力于通过创新为客户提供世界领先的高性能产品和技术。

参考书目

1. *Grand View Research 网站 (*https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-security-market*)*
2. *IN612L 规格书 by InPlay Technologies*