安全硬件系统开发

白皮书

WP100-1.0, 06/28/2019

免责声明

本文档并未授予任何知识产权的许可，并未以明示或暗示，或以禁止发言或其它方式授予任何知识产权许可。除高云半导体在其产品的销售条款和条件中声明的责任之外，高云半导体概不承担任何法律或非法律责任。高云半导体对高云半导体产品的销售和／或使用不作任何明示或暗示的担保，包括对产品的特定用途适用性、适销性或对任何专利权、版权或其它知识产权的侵权责任等，均不作担保。高云半导体对文档中包含的文字、图片及其它内容的准确性和完整性不承担任何法律或非法律责任，高云半导体保留修改文档中任何内容的权利，恕不另行通知。高云半导体不承诺对这些文档进行适时的更新。

摘要

物联网(IoT)引入了大量不同种类的设备，这些设备具有自己独特的系统属性。根据爱立信 2018 年移动报告显示，2018 年实现了 10 亿次蜂窝物联网连接，预计到 2023 年将增长到 35 亿次。这些独特的物联网硬件系统，带来了新一代的安全威胁，攻击者不仅可以访问数据，还可以直接对公共环境中设备进行本地化控制和监控，这可能危及个人安全，甚至是全球安全。

产品安全在生产和采购的各个阶段都存在漏洞。从元器件级上看，器件在工厂测试、封装或装运期间都存在安全风险；从板级来说，最终产品在开发、测试或制造过程中都可能会被篡改或植入漏洞；网络产品制造完成后，器件也可能会被逆向仿制、黑客攻击或克隆。所有这些情况都有可能导致关键数据被访问、监控或控制。

为了避免这些问题，系统中的一个或多个集成电路设备需要建立安全根（Root of Trust，RoT）。这些设备能为系统提供加密功能，可用于安全启动、校验固件、生成或验证密钥、证书、签名以及加密或解密数据。

RoT 设备可以通过安全链为系统的其余部分提供安全功能。从安全的角度来看，它是系统中最关键的设备，因为如果它被攻破，整个系统都会受到威胁。因此，从芯片制造到产品，充分评估 RoT 器件的生命周期至关重要。

加密函数使用密钥对来识别和确认系统功能。生产 IOT 的半导体厂商需要能建立起与 IOT 器件内部的私钥匹配的根密钥。IoT 设备的私钥应该是不可被外界访问的，也不会独立于器件存在。如果私钥在器件制造过程中可被访问，则该器件可能被克隆或攻击。此外，如果密钥存储在器件的 Flash 中或配置信息（Fuse）中，则密钥可能会在芯片制造过程中泄露，或者在产品制造过程中被进行逆向工程和仿制。

为了解决这两个问题，RoT 设备应该具有物理不可克隆功能（PUF）性, SRAM PUF 使用硅元素的某种固有属性作为随机标识符。当设备上电时，可以使用该特性生成密钥对，而不是将其存储在可能被逆向的特定区域。此外，为了防止设备克隆，设备制造商应得到 RoT 设备授权证书。此证书具有基于加密引擎中根密钥对的签名。设备制造商认证授权的签名可以验证设备的真实性，确保 RoT 设备本身不是克隆体。

遵守标准对于确保 RoT 设备中的安全模块与系统的其他部分兼容也很重要。除了遵守国家标准与技术协会(National Institute of standards and Technology)制定的标准外，符合随机数生成标准 SP 800-90，平台固件保护恢复（PFR）标准 SP 800- 193 也是考量安全性和兼容性的重要因素。

安全设备和 RoT 设备选择

对于给定系统中的安全设备一般有两种选择：MCU 和 FPGA。这两种系统各有优缺点。MCU 具有易用性的优势，它更容易获取一些库和应用程序编程接口（API)的授权，且这些库和 API 在器件间更容易移植。比如 FreeRTOS 和 MBED TLS，已被广泛用于嵌入式物联网系统且在此系统中很容易获取 TCP/IP 和 TLS/SSL。MCU 的一个缺点是 IO 数量受限，这可能会限制整个系统安全特性所需的接口数量。另一个缺点是 MCU 不能在运行时检测自身的启动内存。

FPGA 具有 IO 数量多、低延迟和并行检查系统元件的优点。IO 数量多可以控制和监视更多系统元件，低延迟可以更快地检测系统元件，并行计算可以更快地检查整个系统。然而，它的主要缺点是不及 MCU 易用。例如，在没有处理器和大量内存的情况下，FPGA 启用 TCP/IP 和 SSL 堆叠极具挑战性，会使代工（OEM）增加难度。

所以，理想的设备是以低成本和低功耗将安全特性集成到具有 MCU 和 FPGA 结构的设备中。同时，它应具有从边缘设备到服务器的一系列应用所需的封装。这将会提供更优的选择，并根据需要优化系统。利用 FPGA 结构可以实现快速的上电和并行检测，同时利用 MCU 的易用性和库的集成可以加快开发时间。

GOWIN SecureFPGA™-安全 µSoC FPGA，可用于边缘、物联网和服务器系统

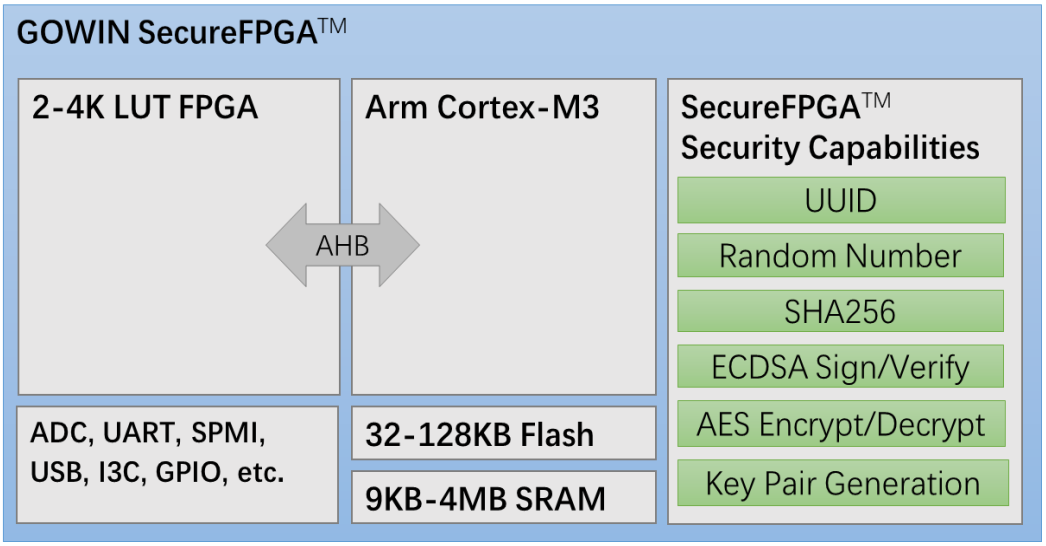
高云半导体利用安全根技术在其 SecureFPGA™产品中实现安全功能，结合 MCU 和 FPGA 的优点，为边缘应用、物联网和服务器应用程序等提供安全保护。SecureFPGA 提供了一个基于 SRAM PUF 技术的安全库，带有 GOWIN 的身份验证，旨在消除从制造到最终产品使用中可能受到的安全威胁。

高云 SecureFPGA™产品封装类型丰富，包括 BGA、QFN 和 TQFP，满足 IoT 和服务器应用需求。IoT 封装 BGA 最小尺寸可以达到 2.5x2.5mm^2。根据不同需求，QFN、BGA 和 TQFP 可用于服务器应用。

全功能安全库

GOWIN SecureFPGA 产品基于物理不可克隆功能（PUF）技术及椭圆曲线加密法(ECC)，集成了功能全面的安全库，旨在解决和消除当前设备存在的安全威胁。此外，GOWIN 还与 Intrinsic ID 合作提供 BroadKey-Pro 安全库。开发人员可以使用加密工具为 GOWIN SecureFPGA 器件中的应用程序创建一个 RoT，或者使用经过验证的成熟的安全解决方案为多设备系统提供一个 RoT。

图 1 GOWIN SecureFPGA™ 器件



GOWIN SecureFPGA™ 安全性能

- 比特流锁定-消除片外读取读取器件比特流可能性
- 工厂设置-激活代码，UUID, CSR 和证书
- 内嵌双启动 Flash –通过固件签名检测进行在线和远程升级
- SRAM PUF –上电时生成的根设备密钥;不存储在 Flash 中
- UUID -使用 SRAM PUF 根密钥对签名的唯一设备标识符
- 设备证书—验证设备为使用 SRAM PUF 根密钥对签名的 GOWIN 设备
- ECDH 加密/解密-基于 ECC 密钥对 AES128/192/256 引擎;基于 SRAM PUF 技术，唯一或随机
- 非对称密钥对生成-基于 SRAM PUF 技术，密钥对唯一或随机
- ECDH 对称密钥生成-基于 SRAM PUF 技术，密钥对唯一或随机
- ECDSA 签名-支持生成和校验
- 随机数生成器-基于 SRAM PUF 和 AES 技术

安全解决方案成熟度及其满足的标准、证书

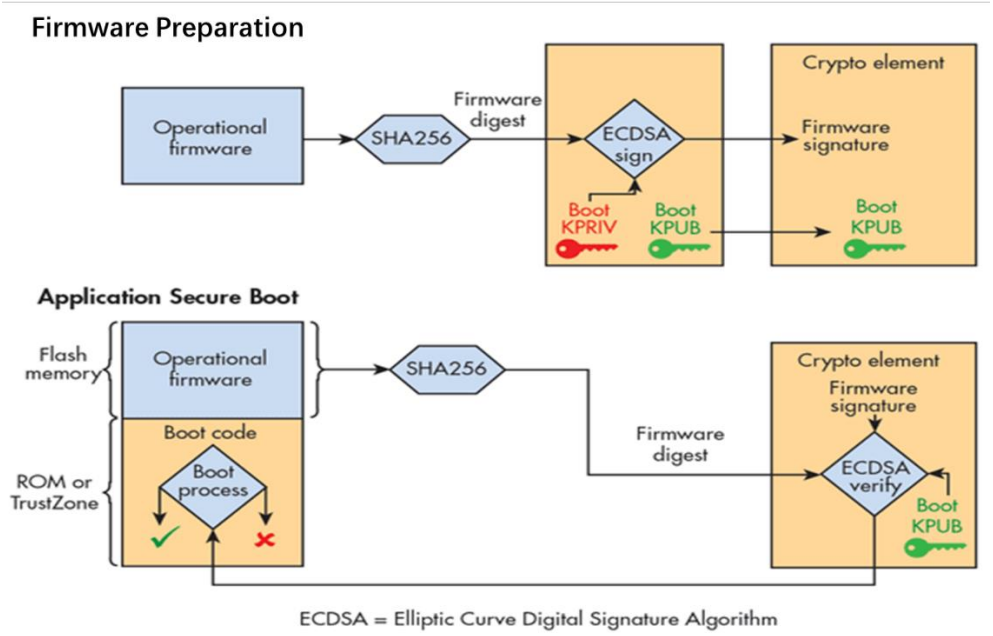
GOWIN 与 Intrinsic ID 合作，在 GOWIN SecureFPGA 设备中植入 BroadKey-Pro 安全库。Intrinsic ID 提供业界最成熟的 SRAM PUF 技术解决方案之一，并已被许多半导体设备供应商采用。多年来，它一直被业界认可，在 2019 年物联网突破奖项中被评为“年度物联网安全产品”。Intrinsic ID 的安全方案已经成功应用在超过 1.25 亿个设备中，满足 FIPS 140-2 附录 B 和中国 OSCCA 标准要求。Intrinsic ID 的安全方案被广泛应用于各个领域，为 RoT 设备提供高标准的安全防护，证书包括 EMVCo、Visa 和 CC EAL6+。

典型应用

安全启动和安全软件更新

安全启动是散列、使用密钥生成签名、然后根据先前创建的签名进行验证的过程。设备可以在运行固件之前检查固件是否被篡改。

图 2 安全启动



对于嵌入式应用，安全启动从使用密钥对的私钥在固件上生成签名开始。此签名存储在设备中，以便在运行时进行比较。一旦生成并存储了签名，一组启动代码就可以使用公钥生成签名，并根据之前生成并存储在设备中的签名对其进行验证。

图 3 SecureFPGA™ - 安全启动准备

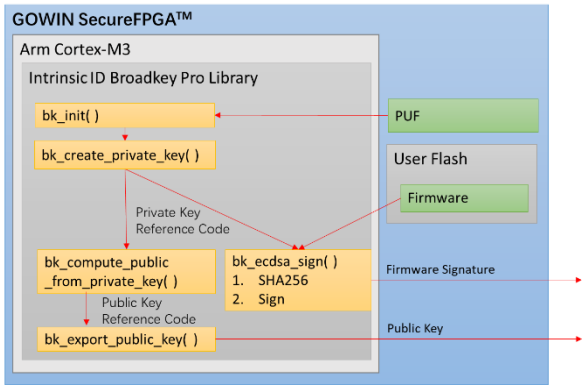
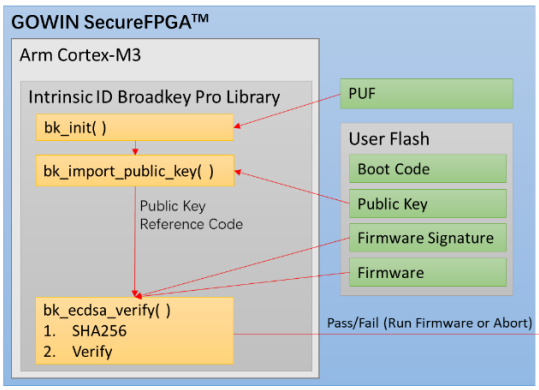
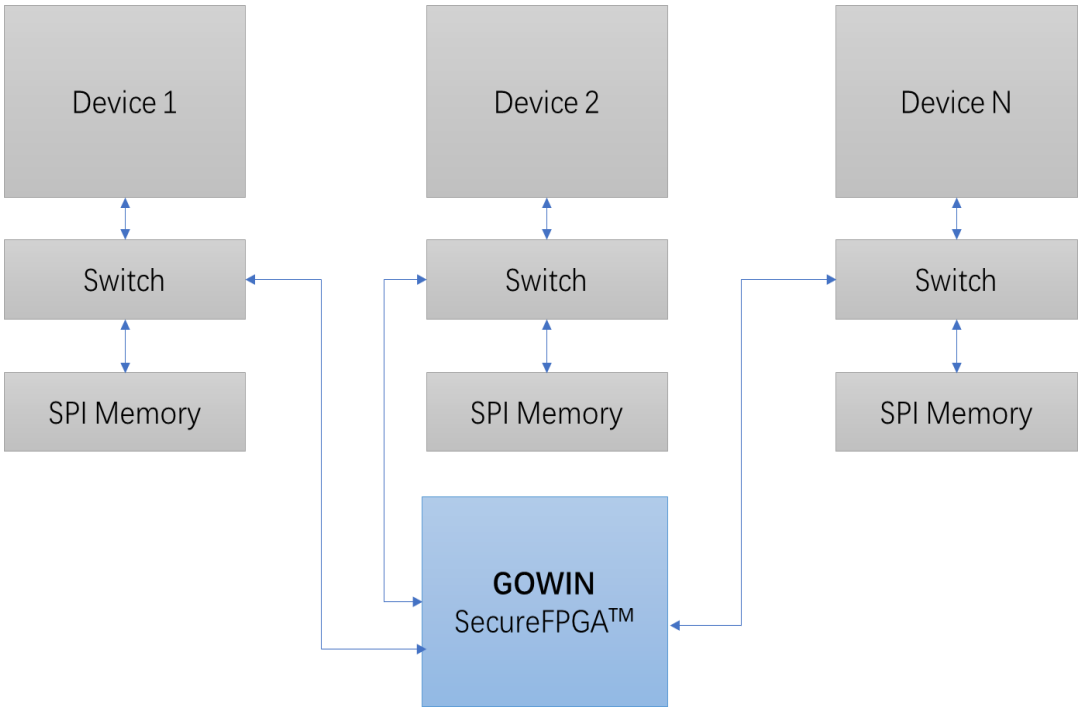


图 4 SecureFPGA™ - 安全启动验证



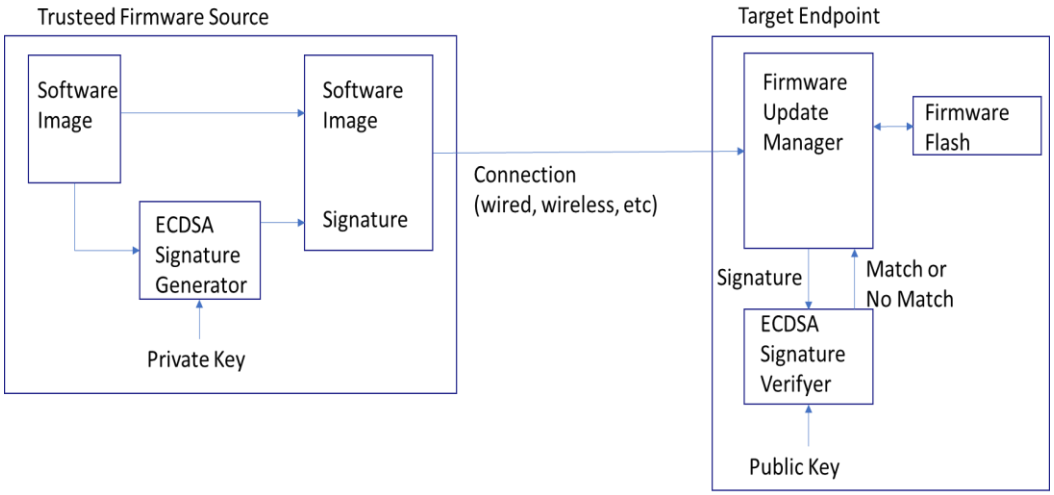
这也适用于验证服务器上多个设备的固件。每个固件都有私钥生成的签名。上电启动时，GOWIN SecureFPGA 产品验证每个设备固件的签名。

图 5 GOWIN SecureFPGA™ 服务器应用的安全启动



除了设备安全启动和服务器应用安全启动外，还可以进行安全固件更新。在这种情况下，固件由源程序签名，并通过某些媒介(如 web 或电缆)发送到设备。设备可以在固件更新前使用公钥验证，或者保留其基础镜像的使用。

图 6 安全固件更新



数据加密

许多应用程序都需要加密数据。例如，一个设备可以单独加密解密其 Flash 或 RAM 中存储的数据或固件，所以不存储明文。另一种情况是，一个设备可以与另一个具有交换密钥的设备交换加密或解密的数据，这些数据在传输过程中不被泄露。

图 7 GOWIN SecureFPGA™ 内部设备加密/解密流程

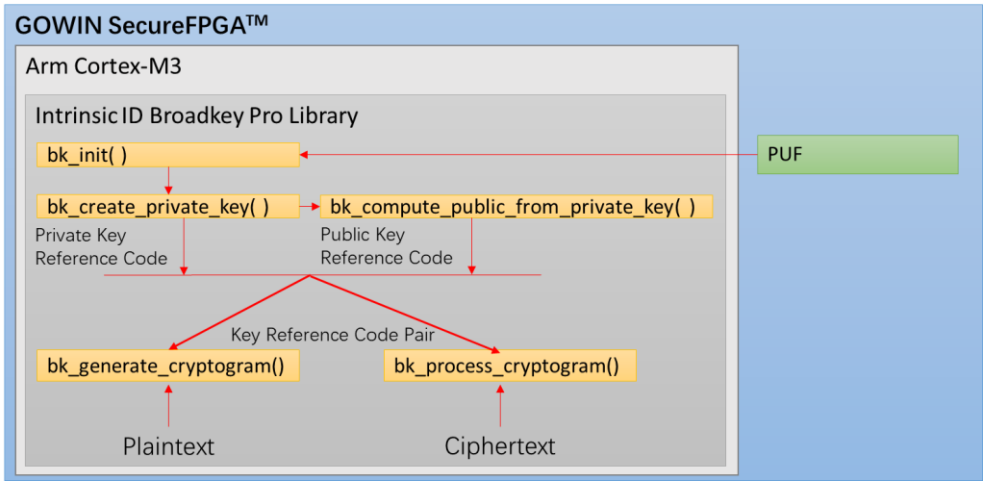
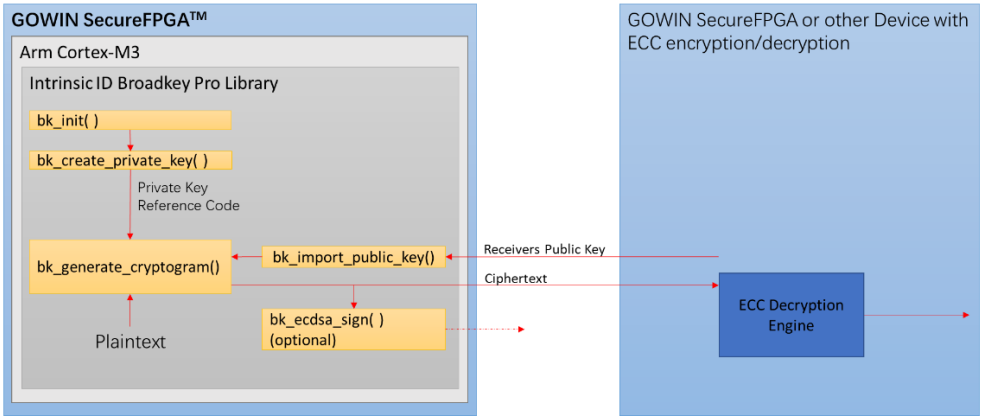


图 8 GOWIN SecureFPGA™ 设备到设备加密/解密流程



工厂制造

为了确保整个制造过程的安全性，高云半导体公司提供了专门的 SecureFPGA 设备。SecureFPGAs 在测试期间提供一个激活代码，该代码允许设备内部始终生成相同的根密钥对。使用 SRAM PUF 引擎生成的根私钥永远不会公开给用户或设备外部。它只对设备内部的安全功能可用，或者用户通过“密钥代码”调用。在配置期间，根公钥从设备导出，形成一个证书签名请求（CSR）或 UUID，可以使用第三方认证授权。GOWIN 提供认证授权(CA)服务为工厂中的每个设备生成证书。GOWIN 的 CA 服务提供了通过验证设备的唯一证书来确认设备是否为正版，如果不是正版，则拒绝使用(详细信息请与高云半导体联系)。这些功能保证了该设备具有唯一的标识，为正版产品，不需要存储数据在 Flash 中，因为从制造到产品生命周期结束期间，Flash 中数据容易泄露。

总结

GOWIN SecureFPGA 产品支持基于 SRAM PUF 技术的安全根。这些设备不会被复制、克隆或预测。这使得它们非常适合于安全密钥的生成和存储、设备身份验证、灵活的密钥供应和芯片数据管理等应用。每个设备都由厂商提供一个唯一的密钥对，该密钥对永远不会公开在设备外部或器件开发、制造过程中。GOWIN SecureFPGA 设备中植入 ID BroadKey-Pro 安全库，可以轻松地将常见的安全特性集成到用户应用程序中。GOWIN SecureFPGA 应用广泛，可以用于各种消费、工业物联网、边缘和服务器管理等应用。

参考资料

1. Columbus, Louis. “2018 Roundup Of Internet Of Things Forecasts And Market Estimates.” Forbes, Forbes Magazine, 18 Dec. 2018, www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#4b33a2747d83.

2. Lazich, Milan. “Intrinsic ID's BroadKey Named 'IoT Security Product of the Year' in 20.” PRWeb, 3 Jan. 2019, www.prweb.com/releases/intrinsic_ids_broadkey_named_iot_security_product_of_the_year_in_2019_iot_breakthrough_awards/prweb16012275.htm.

技术支持

高云半导体提供全方位技术支持，在使用过程中如有任何疑问或建议，可直接与公司联系：

网址：www.gowinsemi.com.cn

E-mail：support@gowinsemi.com

Tel：+86 755 8262 0391


GOWIN高云
智慧逻辑 定制未来