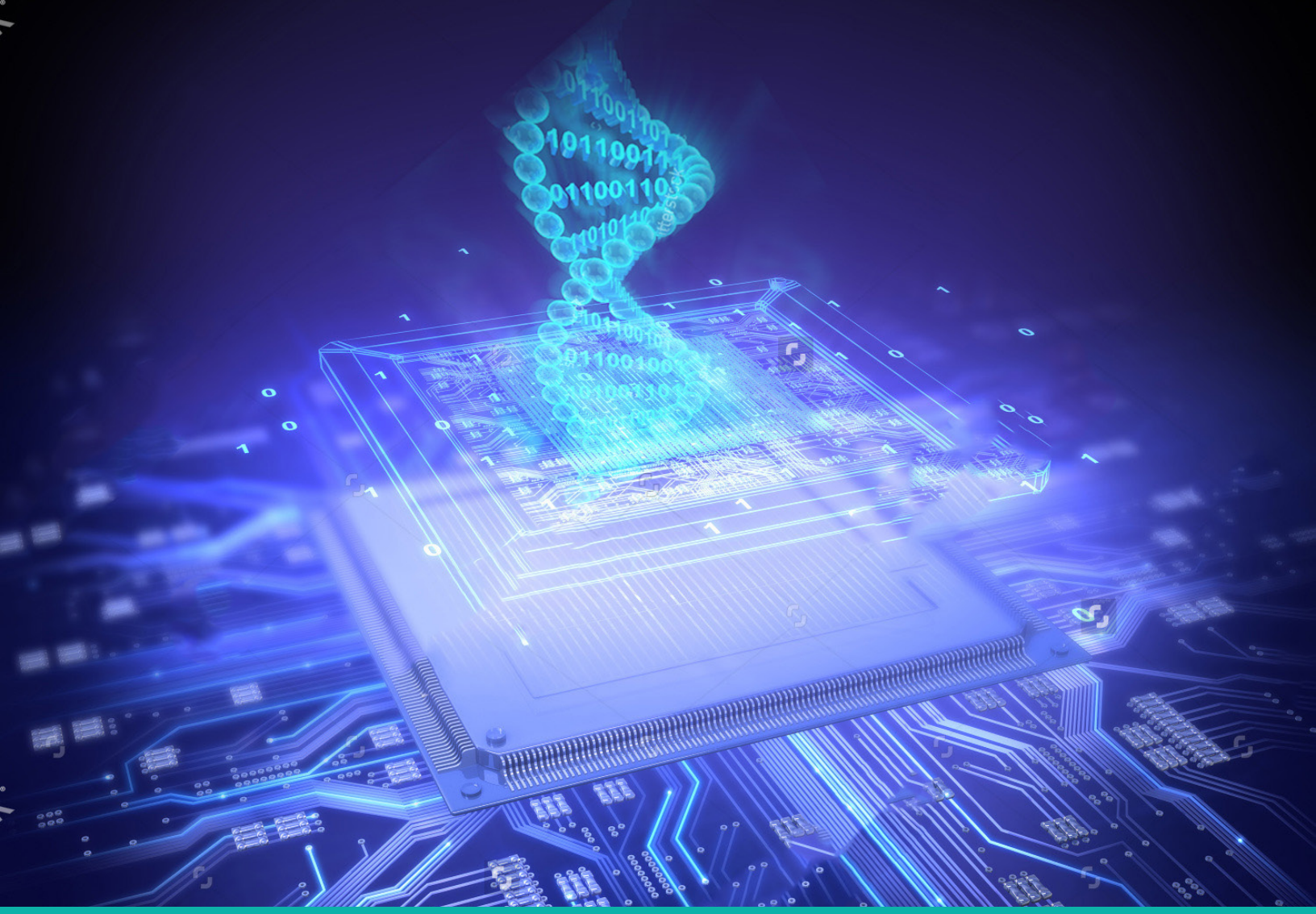

不可复制、完整地嵌入式安全解决方案如何从根本上保护设计

作者：Scott Jones，嵌入式安全部门执行总监，Maxim Integrated

2018年1月

maxim integrated™

摘要

2016年的网络犯罪损失上升24%，超过13.3亿美元，并且这仅仅是美国联邦调查局(FBI)网络犯罪投诉中心跟踪的网络犯罪。关于黑客和其他安全漏洞的新闻头条也屡见不鲜。然而，许多产品制造商仍然将设计安全作为亡羊补牢之举。其中一部分原因可能是误认为实施安全性在时间和资源方面都代价昂贵。本文纠正这些误解并介绍最新的整体式、高成效嵌入式安全，后者为防止入侵提供强有力的保护。

概述

设计安全为什么仍然被忽视?

物联网产品的发展正在超越网络攻击防御水平

去年，电信巨头Telefonica在发布的一份报告中警告说，由于防御网络犯罪的措施仍然落后于物联网(IoT)方案的发展，带来了灾难性后果。

“这不仅仅涉及到数据隐私，或者数字身份的安全。在接下来的几年中，我们的生活将被连接到互联网的设备所包围，这些设备将我们执行的每一步都数字化、将我们的日常活动转化为信息、通过网络分发，并根据这些信息与我们互动。我们的实际生活从来没有如此接近数字世界。”该公司在报告中表示：“范围、规模和风险前所未有：保护物联网。[1]”

然而，安全漏洞仍然有增无减。信用报告巨头Equifax今年夏天发生了大规模数据泄露，黑客获取了美国居民的姓名、社会保障号码、生日、地址及部分信用卡号码，以及英国和加拿大居民的个人数据。今年春天，大规模的勒索软件攻击事件对欧洲、南美洲、亚洲和北美洲的至少150个国家的计算机产生了影响，导致医院、大学、制造商、企业和政府机构出现问题。2016年秋季，由于遭受到基于Mirai恶意软件的僵尸网络攻击，CCTV视频摄像机和DVR造成大面积断网事件。对于每一次广为人知的重大事故，都有许多较小的事件令消费者和企业担心。不言而喻，随着越来越多的产品和系统接入网络，黑客的技术变得越来越高，每个垂直行业都存在亟待解决的风险。例如，请考虑一下以下场景：

- 工业：从之前的孤立系统向现在全部联网的系统过渡，使设备容易受到远程攻击。
- 卫生医疗：该行业存在敏感数据相关的隐私问题、数据完整性问题，以及医疗设备/装置的认证操作。
- 银行：随着网络银行成指数级增长，机构不再能现场保证身份真实性，风险大大提高。
- 零售：移动设备采用开放式架构，但其功能又相当于金融/支付终端，所以必须确保交易和通信安全。
- 通信：端对端安全是防止各种攻击的必要条件。
- 汽车：还记得2015年Jeep汽车被白帽黑客[2]远程控制的事件吗？汽车将很快成为轮子上的计算机，其受攻击风险仍然非常高。

忽视设计安全的风险是巨大的：收入损失、品牌声誉损失，甚至人身伤害。发生破坏之后的亡羊补牢之举往往效果小且见效晚。事实告诉我们，越在设计的早期阶段构建安全性，效果越好。基于硬件的安全已被证明比基于软件的相应措施更有效(关于基于硬件与基于软件的设计安全的比较，请参考白皮书：“为何基于硬件的设计安全性对于所有应用程序都至关重要”)。值得庆幸的是，采用安全IC的硬件方法并不一定需要太多的人力、资源或时间。

上述安全性的代价

虽然您可能面临产品快速上市且要求开发成本足够低的巨大压力，但您认真考虑过破坏造成的相关成本吗？如表1所示的假想终端产品，上述的安全问题最终会带来更多的费用。

基于硬件的安全在一定程度上提供了可靠性，因为网络犯罪分子难以更改设计的物理层。此外，物理层的存在使得恶意软件不可能渗透操作系统并潜入设计的虚拟层。从设计周期之初开始，即可将安全性整合到设计的底层以及后续所有层。

利用安全IC，例如从内部、不可变存储器中执行代码的微控制器，防止试图破坏电气器件硬件的攻击。微控制器的ROM储存被认为是“信任根”的启动代码，因为代码不可修改。因此，这种“不可更改”、受信任的软件可用于验证和认证应用软件的签名[3]。利用从底层就基于硬件的“信任根”方法，可将设计的更多潜在进入点关闭。

忽视设计安全导致财产损失

无安全IC	
10 Mu销售量@ $10	$100M
假冒产品低于15%	**-$15M**
销售净额	**$85M**
产品成本：10Mu @	-$30M
利润	**$55M**

使用安全认证器@$0.50	
10 Mu销售量@ $10	$100M
假冒产品小于 0%	$0M
销售净额	**$100M**
产品成本：10Mu @	-$35M
利润	**$65M**

表1. 假冒伪劣带来的资产损失最终远远超出实施安全性所需的成本。

安全认证器是高成效的IP保护措施

安全微控制器和安全认证器等嵌入式安全IC提供整体方案，保护从每个传感器节点到云端的整个系统。然而，并非所有安全IC都是相同的。例如，由于成本、功耗以及要求复杂的固件开发，有些安全微控制器就不适合IoT设备或端点。于是出现了一些加密控制器能够实施嵌入式、联网产品的完全安全性，且无需任何固件开发工作，例如，Maxim的MAXQ1061 DeepCover®器件。作为协处理器应用于初始设计，或者整合到已有设计，保证数据保密性、身份真实性和设备完整性。

对于安全认证器，器件应提供一组核心的固定功能加密操作、密钥存储以及其它适合IoT和端点安全的相关功能。凭借这些能力，安全认证器即可保护IP、防止克隆以及对外设、IoT设备和端点进行安全认证。Adevice such as Maxim's DS28C36 meets these needs.

在评估嵌入式安全技术时，还应该考虑哪些因素？内置加密引擎和安全引导加载程序的安全微控制器，可有效防止密码分析攻击、物理篡改和反向工程化等威胁。Design SHIFT是一家总部位于美国加利福尼亚州门洛帕克市的数字安全和消费产品工程公司，其ORWL安全台式计算机需要此类特性。该公司设计ORWL时，要求安全认证和防止物理攻击两种功能，需要强壮的信任根安全。Design SHIFT找到了所需的方案：MAX32550 DeepCover ARM® Cortex®-M3安全微控制器。

“许多软件人员说，一旦您失去对硬件的控制，您就玩完了”。Design SHIFT公司的CEO Olivier Boireau表示：“建立信任根是强壮保护的保证。”

通过物理不可复制特性(PUF)技术增强保护

我们开始在安全IC中看到一项更高级的加密技术，即物理不可复制特性(PUF)。PUF依赖于IC器件的复杂且可变的物理/电学特性。由于PUF在制造过程中产生的随机物理因素(不可预测、不受控)，实际上不可能复制或克隆[4]。集成PUF技术的IC带有与生俱来的数字指纹，可用作唯一的密钥/密码，支持提供安全认证、识别、防伪、硬件-软件绑定以及加密/解密的算法。

Maxim的PUF电路依赖于基本MOSFET器件模拟特性来产生密钥，而器件的模拟特性是自然随机发生的；该方案被称为ChipDNA™技术。这种专利方法可确

保PUF电路产生的唯一二进制数值，在随温度和电压变化以及器件老化的情况下保持不变。高水平的安全性在于该唯一的二进制数值实际上未储存在非易失存储器芯片的任何位置，而是需要时由PUF电路生成，使用后立即消失。因此，与之前的安全器件容易遭受对非易失存储器的侵入式物理攻击从而获取密钥不同，基于PUF的器件不容易受到这种类型的攻击，因为本来就无密钥可偷。此外，如果基于PUF的器件遭受侵入式物理攻击，攻击本身会造成PUF电路的特性发生变化，进一步阻碍这种类型的攻击。ChipDNA PUF技术已证明其在生产工艺、电压、温度和老化方面的优异可靠性。此外，对基于NIST[6]的随机性测试结果的PUF输出评估已经成功完成，结果合格。图1所示为ChipDNA PUF技术的不同用途：内部存储器加密、外部存储器加密和安全认证密钥生成。

第一款采用PUF技术的安全认证器

Maxim第一款采用ChipDNA PUF技术的安全IC为DS28E38安全认证器，设计用于提供高成效的入侵式物理攻击防御。DS28E38 (图2)提供：

- 基于FIPS186 ECDSA的质询/响应安全认证
- ChipDNA安全存储数据，可选的ECDSA-P256私钥数据源
- 2Kb EEPROM阵列，用于用户存储器和公钥证书

信任根不可篡改

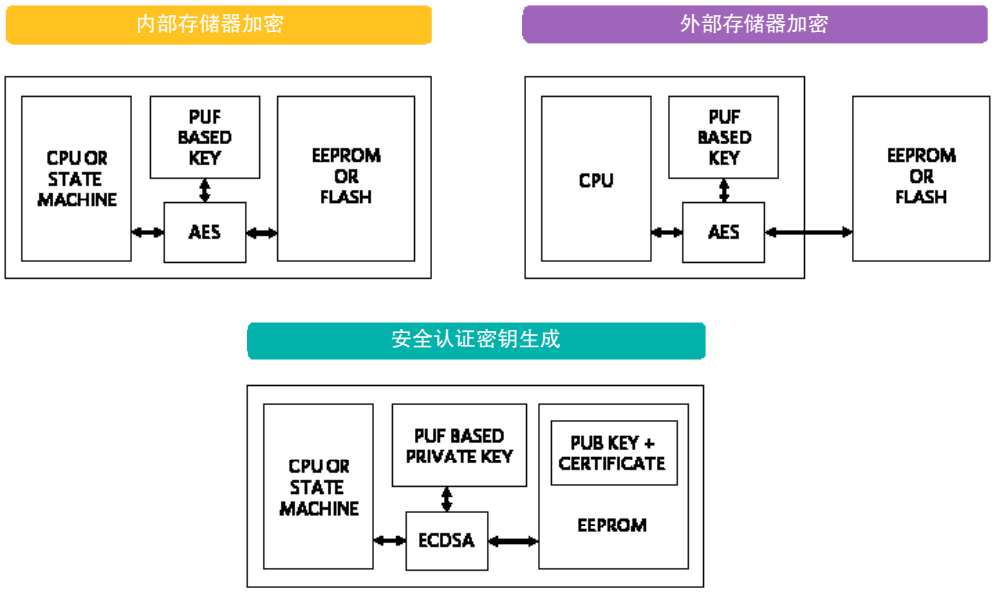

图1. ChipDNA PUF技术的不同用途。

- 带认证读取的仅递减计数器
- 唯一的工厂编程只读序列号(ROM ID)
- 单触点、1-Wire®寄生接口，提供通用、坚固且非常可靠的互连方法，实现在之前无法实现的领域进行安全认证。

DS28E38只是第一款采用ChipDNA PUF技术的产品。Maxim正在增强其整个嵌入式安全产品线，包括安全认证器和安全微控制器，将在未来几个月内提供多款采用ChipDNA技术的新产品。

PUF技术无密钥可偷

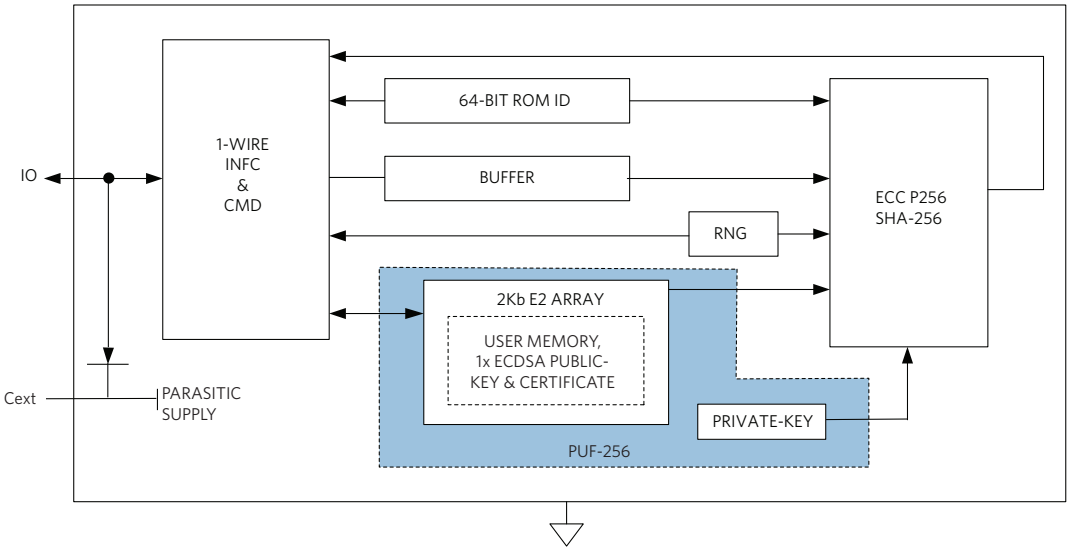

图2. 带ChipDNA PUF保护的DS28E38 DeepCover安全ECDSA认证器方框图

总结

当今的嵌入式安全IC提供整体式解决方案，从一开始就可以采用多级安全措施保护您的设计，支持加密算法，篡改检测以及其它诸多保护。特别是PUF技术，提供极其强大的机制防止侵入式和非侵入式攻击。无论如何，你无法盗窃一个并不存在的密钥。

更多信息

阅读嵌入式安全方案指南，了解更多关于可保证您下一代设计安全性的嵌入式安全方案。

来源：

[1] https://www.telefonica.com/documents/737979/5540857/Telef%C3%B3nica_Security_IoT_Final.pdf/a28293d4-f15a-4f21-8353-317faf892a18

[2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] http://www.embedded.com/design/safety-and-security/4438300/Securing-the-IoT--Part-2---Secure-boot-as-root-of-trust-

[4] https://en.wikipedia.org/wiki/Physical_unclonable_function

[5] http://rijndael.ece.vt.edu/puf/background.html

[6] https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software