INTRINSIC ID

安全的硅指纹

1 总述

多年来，基于硅的物理不可克隆功能 （PUF）被视为一个充满希望和创新的正在稳步发展的安全技术。同时，低成本和强大的密钥存储技术，对于实现负担得起的、有效的安全系统也至关重要。如今，Intrinsic ID 的基于静态随机访问存储器 （SRAM） 的 PUF 提供一个成熟和可行的安全部件，正在广泛被用于商业产品中。它们被运用于从微型传感器和 MCU 到高性能现场可编程门阵列 （FPGA） 以及保护金融交易、用户隐私和军事机密的安全元件等各种设备中。

Intrinsic ID 是一家 2008 年从飞利浦电子分拆出来而成立的、总部和研发都位于荷兰埃因霍温的高科技公司，一直专注于研究基于 SRAM 的 PUF 技术，并将其产品化，在过去的 10 多年里得到了广泛的应用。

2. 基于 SRAM 的 PUF

由于深度亚微米制造工艺的变化，集成电路（IC）中每个晶体管的物理性能略有不同。这将导致电子特性（如晶体管的阈值电压和增益系数）方面的微小而可衡量的差异。由于这些工艺变化在制造过程中不能完全控制，因此无法复制或克隆这些物理设备属性。

阈值电压易受温度和电压等环境条件的影响，因此其值不能直接用作唯一的密钥或标识符。

另一方面，SRAM 单元的行为取决于其晶体管的阈值电压的差异。即使是最小的差异也会被放大，并将 SRAM 单元推入两种稳定状态之一。因此，其 PUF 行为比基础阈值电压稳定得多，这使它成为使用阈值电压构建标识符最直接和最稳定的方法。

3. 基于 SRAM 的 PUF 的行为

SRAM 存储器由许多 SRAM 单元组成。每个 SRAM 单元由两个交叉耦合反向器组成，每个反向器都由 PMOS 和 NMOS 晶体管构建。当电压施加于 SRAM 单元时，其逻辑状态由反向器中 PMOS 晶体管的阈值电压之间的关系决定。首先开始导通的晶体管决定结果，即逻辑的"0"或"1"。

事实证明，每次 SRAM 上电时，由于阈值电压的随机差异，每个 SRAM 单元都有其自己的偏向的状态（“0”或者“1”）。这种偏向性与相邻单元的偏向性无关，也与单元在芯片或者晶圆上的位置无关。

因此，一片 SRAM 区域生成 0 和 1 的独特随机分布。此分布可以称为 SRAM 指纹，因为它对每片 SRAM 是唯一的，因此对每颗芯片芯片也是唯一的。于是，它可以被用作 PUF。

从 SRAM PUF 派生的密钥不会"在芯片上存储"，而是"从芯片"中提取，当需要时，就实时从芯片中提取出来。这样，它们只在很短的时间内出现在芯片中。当 SRAM 未通电时，芯片上不存在密钥，使解决方案非常安全。

下图 1 大致展示了其行为：

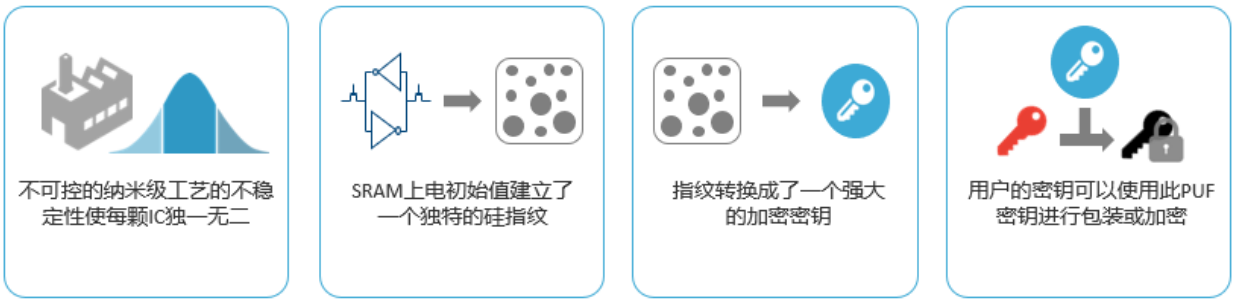

图 1. 从 SRAM 的行为中提取出一个强大的密钥

4. 基于 SRAM 的 PUF 的可靠性

决定 PUF 行为的深亚微米工艺变化在制造过程中被固定下来，之后不会更改。因此，SRAM 单元的上电初始值的偏向性是长期的，并且是稳定的。

然而，仍然有一定程度的噪音。有少数单元的阈值电压是接近平衡的，因此其上电初始值是不稳定的，看起来是随机的，不带偏向性。因此，对于一片 SRAM，每次上电启动时，会出现一个略有不同的初始值，我们将这不同的部分称作噪声。此噪声取决于温度、电压斜坡和工作条件。

基于 SRAM 的 PUF 响应的噪声已经在各种环境和制造工艺中进行了详尽的特征描述和测试：

- 温度范围从 -55°C 至 +150°C（-67°F 至 300°F）
- 电压变化 +/-20%
- 湿度高达 80%
- EMC 测试 3V/m（EN55020 0.15~150 MHz 和 IEC 61000-4-3 80-1000MHz）

特别值得一提的是，基于 SRAM 的 PUF 已经通过与客户和合作伙伴的合作，获得了汽车、工业和军事用途的资质，在这些领域已经被广泛使用。

我们已经对其进行了数百万次的测量。在所有这些情况下，基于 SRAM 的 PUF 响应的平均噪声水平被发现低于 15%。尽管有这么多的噪声，但每次为 SRAM 供电时，它都有可能重建一个高熵的、设备唯一的、可靠的密钥。这可以通过应用纠错技术（如 “辅助数据算法” （参考文献一）)或 “模糊提取器” （参考文献二））来实现。这些算法执行两个主要功能，即纠错和隐私放大，这将在下面进行解释。

5. 纠错

加密密钥重建的纠错技术需要两个阶段：注册阶段和重建阶段。在注册阶段（一次性过程），PUF 响应映射到纠错代码的码字。有关映射的信息存储在激活码 （AC） 或辅助数据中。AC 的构造使它不会泄漏任何有关密钥的信息。它应该存储在 PUF 算法可以访问的存储器中，但它可

以存储在芯片外，因为它不敏感、不用保密。任何对 AC 的更改，无论恶意与否，都将阻止密钥重构。每一个 AC 只对创建它的芯片有效。

每次设备运行身份验证协议并需要 PUF 密钥时，都将重新进行包含有噪声的 PUF 测量，并从 AC 和这个新的 PUF 响应中提取 PUF 密钥（无噪声）。这被称为重构阶段。注册阶段和重构阶段如图 2 所示。

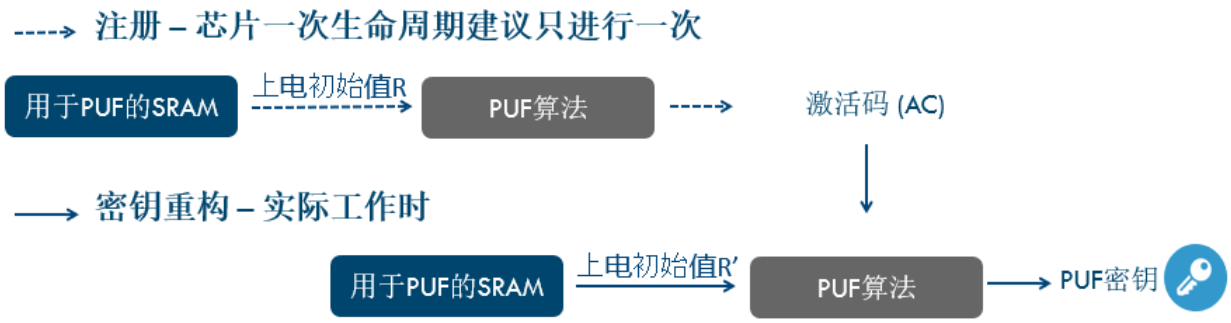

图 2. PUF 密钥生成的注册和重构阶段（注意，R 是注册时的初始 PUF 响应，而 R' 是带有噪声的重构时的 PUF 响应）

纠错算法的设计使密钥重构的平均错误率小于 10^{-12}。即使在极端情况下，例如极端温度下，即使噪声水平上升至 25%，重构的错误率仍然低于 10^{-9}。

6. 隐私放大和安全

密钥是完全随机的，因此是不可预测的，基于这一事实，密钥提供了安全性。物理测量（如 PUF 响应）具有高度的随机性，但通常不是完全均匀随机的。隐私放大用于生成均匀随机密钥。

通过结合纠错和隐私放大，一个 1kByte 的 SRAM PUF 响应可以转换成为 256 位均匀随机密钥，而对于转换一个具有完全随机的 128 位密钥只需要大约 0.5 kByte。

一个典型的 SRAM PUF 包含如此多的熵，仅需要几十个字节就可以提供一个不重复的全局唯一标识符，该标识符可用作唯一（但有噪声的）电子芯片 ID （ECID） 或序列号。

客户的专门的安全实验室和安全团队分析了 Intrinsic ID 的 SRAM PUF 针对各种侵入性和非侵入性物理攻击的安全性，而没有暴露任何弱点。用扫描电子显微镜、激光、FIB（聚焦离子束） 和探针攻击都没有成功。侧信道攻击没有导致任何敏感信息的泄漏。

7.老化

在基于 SRAM 的 PUF 上进行了加速老化试验，以研究随着时间推移的噪声水平的情况。通过使用抗老化专利技术，基于 SRAM 的 PUF 技术可以保证 25 年的使用寿命（参考文献三）。

8. 实现 —— 软件版本 BK 与硬件版本 QuiddiKey

Intrinsic ID 将上述纠错、随机性提取、安全对策和抗老化技术捆绑在其产品中。它们以非常安全的方式从 SRAM PUF 中提取加密密钥，既有称为 QuiddiKey® 的硬件 IP 版本（RTL 源代码），也有称为 BK™的软件 IP 版本（二进制库文件），还有软件、硬件相结合的混合版本。当已经集成的硬件加速器（如 对称加密算法、非对称加密算法）与 SRAM PUF 技术结合使用时，这些结合硬件和软件的混合解决方案可以极大的提高效率。

硬件 IP 面积小且速度快，大约为 2.5 万门、5 万个时钟周期，可连接到公共互连总线上，如 AMBA@AHB、APB 以及专有接口。逻辑中包含内置的自测试 （BIST）、诊断和运行状况检查。并且提供了驱动程序以方便与软件的集成。由于它是纯数字的，单时钟域逻辑电路，它很容易被综合到任何目标工艺库上。

软件参考实现最小、最基础的功能版本可以小到只有 4KBytes，可用于任何主流的平台，如 ARM ®、ARC ®、英特尔®、MIPS 和 RISC-V。软件实现可用于通过固件升级的方式将 PUF 技术部署到现有产品中。Intrinsic ID 还提供与 Arm@TrustZone 预先集成的 BK 版本。

QuiddiKey 硬件和 BK 软件解决方案都可以根据应用进行优化，以实现低内存占用、低延迟或低存储空间使用。重用或与现有的密码内核和随机数发生器集成可以进一步提高性能并减少占用空间。Intrinsic ID 解决方案附带了全面的产品规范和集成指南，包括说明了提供给应用程序程序员的 API 使用方法的参考代码。

9. 使用条件与要求

这些 Intrinsic ID 的产品使用未初始化的 SRAM。这可以是一个单独的 SRAM 块，也可以是一个较大的现有 SRAM 的一部分。标准的 SRAM 就足够了。要存储激活码 （AC），需要访问存储介质，它可以是嵌入非易失性内存 （NVM），也可以是电路板上的独立存储器，例如闪存或云存储。对于软件版本 BK，需要知道处理器的具体型号以及其具体所使用的 C 语言编译器。PUF 算法可以存储在任何 NVM 中，例如 flash、ROM。

另外，还需要说明的是，SRAM 在几乎所有的 MCU 和 SoC 中都有集成、在芯片制造工艺的每个工艺节点都存在、并且是标准制造流程的一部分。使用基于 SRAM 的 PUF 技术也无需进行耗时的评估和芯片测试，因为 Intrinsic ID 及其合作伙伴的广泛测试已经表明，该技术能够可靠地扩展到当前可用的最小工艺节点。

10. 实际使用情况

基于 SRAM 的 PUF 已经被很多半导体公司采用、并且产生已经在市场上大量销售多年。它们已经广泛应用于微控制器、FPGA 和智能卡控制器中（参考文献四）。在其他市场，软件版本（BK）的实现使该技术能够快速部署，甚至可以作为一种在现有硬件基础上进行安全功能改进的解决方案。Intrinsic ID 与领先的半导体公司合作，开发了用于保护嵌入式系统、传感器和控制器的解决方案。有关我们的 SRAM PUF 部署的详细信息，请访问我们的网站：https://www.intrinsic-id.com。

11. 结论

基于 SRAM 的物理不可克隆函数已成功在商业产品中实现。SRAM PUF 结合了高安全性和可靠性与低成本、低空间占用、并且易于实现的特点。它们已经被广泛部署在从 MCU 和传感器到高性能 FPGA 和安全芯片等等许多设备中。

许多实现一致地证明了该技术的可靠性和安全性。SRAM PUF 是一项成熟而强大的技术，专为安全性而设计，并基于坚实的理论基础。SRAM PUF 已经在高安全市场中赢得了信誉，现在正在从低成本 IoT 应用到政府、国防和支付行业的高端安全解决方案等市场中越来越多地受到关注和使用。

参考文献一：J.-P. Linnartz and P. Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric templates,” in International Conference on Audio and Video-based Biometric Person Authentication (AVBPA’ 03), ser. LNCS, J. Kittler and M. S. Nixon, Eds., vol. 2688. Heidelberg: Springer-Verlag, 2003, pp. 393–402.

参考文献二：X. Boyen, “Reusable cryptographic fuzzy extractors,” in ACM Conference on Computer and Communications Security (CCS’ 04). New York, NY, USA: ACM, 2004, pp. 82–91. AND Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in EUROCRYPT’04, ser. LNCS, C. Cachin and J. Camenisch, Eds., vol. 3027. Heidelberg: Springer-Verlag, 2004, pp. 523–540.

参考文献三：R. Maes and V. van der Leest, "Countering the effects of silicon aging on SRAM PUFs", Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST), pp. 148-153 available at http://www.Intrinsic.id.com/wp-content/uploads/2014/09/PUF_aging.pdf

参考文献四：H.Hodson – New Scientist, “Silicon fingerprint on chips could make any gadget unhackable” June 6, 2016 https://www.newscientist.com/article/mg23030771-400-physical-quirks-in-silicon-chips-are-key-to-unhackable-devices/ or “Chip design quirks make our lives more secure” in the June 11 printed issue page 24.

info-china@intrinsic-id.com www.intrinsic-id.com INTRINSIC ID

Intrinsic ID Inc., 710 Lakeway Drive, Sunnyvale, CA 94085 U.S.
Intrinsic ID B.V., High Tech Campus 9, 5656 AE Eindhoven, The Netherlands