

物理不可克隆函数综述

张紫楠*, 郭渊博

(信息工程大学 电子技术学院, 郑州 450004)

(*通信作者电子邮箱 zzn20063063@126.com)

摘要: 尽管物理不可克隆函数(PUF)是近年来刚刚提出的概念,但由于它在系统认证和密钥生成等安全方面的潜在应用前景,已成为硬件安全领域研究的一个热门话题。为了系统得到 PUF 的全貌,以便在以后的研究和开发中更好地理解 and 应用 PUF。首先,根据迄今为止研究人员提出的 PUF 的各种不同实现方法,分类概括出其详细的设计,并总结出当前仍然面临的一些问题;然后,综合这些不同的设计和实现方法的定义,归纳出覆盖 PUF 共同特性的属性集并讨论了其各自的内涵;最后,从密码学应用的角度,讨论了 PUF 的应用方向,并展望了关于 PUF 未来的几个有意义的研究方向。

关键词: 物理不可克隆函数;认证;密钥生成

中图分类号: TP393.08 **文献标志码:** A

Survey of physical unclonable function

ZHANG Zi-nan*, GUO Yuan-bo

(Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan 450004, China)

Abstract: Though PUF is a new concept in recent years, since it has application prospect for the security of system authentication and key generation, it has become a hot research topic in the field of hardware security. In order to get the whole picture of physical unclonable function for better application in the future research work, first, based on the the different PUF implementations available, this paper classified the detailed design, and summed up the main problems. Then based on these categories, this paper proposed a non-formal property description. Next, from the point of view of cryptographic applications, this paper summarized the PUF application. Finally, this paper pointed out a few meaningful PUF future research directions.

Key words: Physical Unclonable Function (PUF), authentication; key generation

0 引言

近些年来,随着智能卡、射频识别(Radio Frequency Identification, RFID)等物理实体的广泛应用,如何对这些物理实体实施有效认证是成为确保系统安全的基础问题。然而,由于这类实体普遍存在着计算能力差、资源有限等问题,传统基于密码学的认证方法在应用时存在着很大障碍。借鉴当前普遍使用的人体唯一特征(指纹或虹膜)对个人实施认证的思想,人们基于物理实体的内在物理构造来唯一地标识单个物理实体实现有效认证的思路,提出了物理不可克隆函数(Physical Unclonable Function, PUF)的概念。PUF是指对一个物理实体输入一个激励,利用其不可避免的内在物理构造的随机差异输出一个不可预测的响应这样一个物理不可克隆的函数。PUF最基本的应用是利用实体的唯一标识来实现认证^[1],随着人们对 PUF 的理解和应用的不断深入,PUF 又逐渐被应用到系统认证、密钥生成等更多的领域,并逐渐成为硬件安全领域研究中的一个热门话题。

为了使 PUF 真正具有物理不可克隆性等特性, Pappu 等^[2]首先正式给出了 PUF 的概念,并设计实现了光学 PUF 来实现系统认证等应用。自此,朝着实现方法和应用多样性的

方向,人们提出了越来越多新类型的 PUF 实现方法,如涂层 PUF^[3]、基于仲裁器的 PUF^[4-5]、蝴蝶 PUF^[6]等,并且基于这些实现方法实现提出越来越多新的安全应用如知识产权(Intellectual Property, IP)保护^[7]、系统认证^[8-9]、可信计算^[10]和密钥生成^[11-12]等。

从信息技术进化的角度来看,PUF 的使用至少有两个优势:首先,计算和通信设备往往变得更小,并且其深度整合会导致很多额外的物理的相互影响。在这种情况下,自然地利用设备的物理性质,而不是刻意地消除这种影响会给系统减少很多额外的开销。同时分布式(例如云)计算的日益发展和“物联网”的兴起使越来越多的数十亿的对象互联也创建了一个重要的信任与安全的挑战。在这种情况下,给每个对象或计算设备装备一个唯一身份,可以作为更高水平安全架构的信托锚(trust anchor)来使用。

当前,尽管 PUF 已经得到越来越多的研究人员的关注,但这方面的研究工作刚刚开展不久,相关的研究成果还不是很系统。为了在现有成果基础上对 PUF 的概念和特性进行比较详细的刻画,以便在以后的研究和开发中更好地理解 and 应用 PUF,这里尝试对 PUF 进行综述。

收稿日期: 2012-05-28; 修回日期: 2012-07-11。 基金项目: 河南省科技创新杰出青年计划项目(104100510025)。

作者简介: 张紫楠(1987-),男,辽宁葫芦岛人,硕士研究生,主要研究方向:网络安全; 郭渊博(1975-),男,陕西周至人,副教授,博士,主要研究方向:网络与通信、信息与网络安全。

1 PUF 实现方法

自从 Pappu 等^[2]正式提出 PUF 的概念以来,人们提出了许多基于各种实现技术的新类型的 PUF 实现方法。本文根据电路技术,归类总结出三类,即非电子 PUF、模拟电路 PUF 和数字电路 PUF。目前提出的大部分 PUF 的实现方法可基本上归类如图 1 所示。

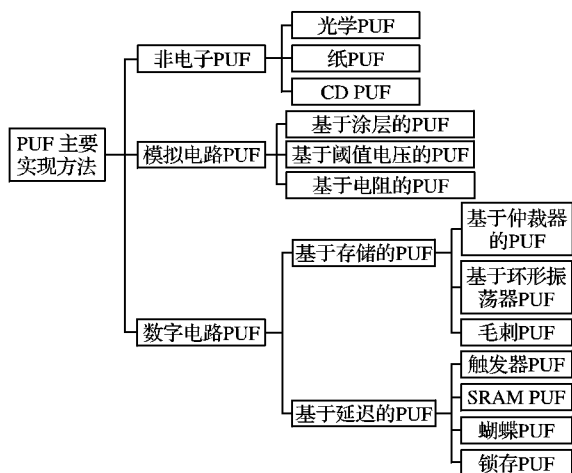


图1 目前提出的主要 PUF 实现方法

非电子 PUF 中最具代表性的是 Pappu 等提出的光学 PUF^[2],它也是在安全应用中 PUF 概念的第一个正式描述。光学 PUF 的核心组件是一个随机掺杂光散射粒子的小光透明令牌,当用一个激光照射光透明令牌的时候,它就能辐射出一个有明暗斑点的复杂图像,即散斑。一个贾柏滤波器可以很好地提取这样一个散斑,并输出光学 PUF 的一个响应。所以在光学 PUF 中,激光的物理参数是激励,而滤波器的输出是响应。由于激光和散射粒子相互作用的复杂性质,响应被认为是高度随机和唯一的。光学 PUF 的响应依赖于光令牌的微观物理细节,这就会导致两个同样产生的令牌将显示出一个根本不同的激励响应行为,从而防止克隆的发生。此外,文献[2]中提出令牌的一个小的物理变化例如钻微孔等,将会大大改变 PUF 的激励响应行为,也就是实现防篡改属性。其他的非电子 PUF 包括在文献[13]中 Bulens 等提出的纸 PUF 的概念,它的主要原理是利用纸文件不规则的纤维结构的激光反射来作为防止伪造的“指纹”。在文献[14]中, Hammouri 等提出了 CD PUF 的概念,它的主要原理是在 CD 制造过程中,可变因素会影响平坦面的精确长度和光盘的坑,这可以被用来提取 CD 的“指纹”。

模拟电路 PUF 中最具代表性的是 Tuyls 等提出的涂层 PUF^[3]。它的原理主要是通过集成 PUF 到集成电路(Integrated Circuit, IC)上来实现。在一个 IC 上喷上一种特殊的涂层,这种涂层包含一些小的随机的介质颗粒。在 IC 顶部的金属层上有电容式传感器,它用来测量介质造成的随机电容。当在 IC 上喷上这种涂层的时候,不同的电容式传感器就会测量这个涂层造成的随机电容,然后输出涂层 PUF 不同的响应。所以在涂层 PUF 上,电容式传感器是涂层 PUF 的激励,而介质造成的随机电容是涂层 PUF 的响应。其他的模拟电路 PUF 包括 Guajardo 等^[15]提出了一个类似于涂层 PUF 的

概念,叫作 LC-PUF。在文献[16]中, Lofstrom 等通过芯片上的模拟测量电路直接测量 MODFET 的阈值电压变化来实现一个 PUF 的功能。在文献[17]中, Helinski 等介绍了一种基于电阻值来识别一个 IC 电源分配系统的方法。

数字电路 PUF^[7]除了具有 PUF 本身的条件外,还需要满足两个额外的要求:

1) 一个完整的 PUF 要完全集成到嵌入式设备中,这里完整的 PUF 是指它包括实现 PUF 的完整设备如测量设备等;

2) 标准的设备制造流程可以完全地执行这种集成,即不需要特定的 PUF 过程步骤或组件。

很显然,数字电路 PUF 可能提供更高的安全条件,但也有可能需要更多的实现成本。大部分数字电路 PUF 的实现方法都是基于数字集成电路提出的。其主要的工作原理是,在同样的生产条件下,IC 之间会产生不可避免的随机制造差异,利用这个差异就可以实现数字电路 PUF。数字电路 PUF 目前主要有两种主要实现方法:

1) 利用数字信号的传播延迟变化来实现。一个数字信号的传播延迟就是信号在路径上遇到元器件电子参数的一个函数。这些元器件的电子参数例如 MOSFET 通道长度、宽度^[18]和阈值电压^[19]、氧化层厚度、金属线的形状^[20]等都会受到制造差异^[21-22]的影响。因此,一个数字信号的传播延迟将会有部分随机性,并且在测量时显示出类似于 PUF 的行为。目前有三种主要的具体实现方法,即基于仲裁器的 PUF^[4-5]、基于环形振荡器的 PUF^[23-24]和基于毛刺的 PUF^[25]。基于仲裁器 PUF 的主要原理是在 IC 上实现两个对称的数字信号延迟路径,一个激励控制着选择路径的确切延迟。引入判决条件是通过两个脉冲同时在两个路径上走,看哪个路径更快并相应地由仲裁器电路输出一位响应。基于环形振荡器的 PUF 使用负反馈转化数字信号为振荡指标,通过测量振幅,就可以获得测量的延迟。这两种具体的实现方法都是在集成电路上实现和测试的,并且能够显示出一个很好的 PUF 行为。在文献[25]中 Suzuki 等提出了另一种利用延迟路径差异的 PUF,叫作基于毛刺的 PUF。毛刺的部分随机性是由于不可避免的制造差异引起的,所以通过观察一个随机逻辑电路的毛刺就可以显示出一个 PUF 的行为。

2) 利用一些存储器单元结构的稳定状态的制造变化来实现。一般情况下,完成存储器的数字存储是通过双稳态逻辑单元,也就是一个逻辑单元假设有两个不同的但是逻辑上稳定的状态。具体过程是,首先通过交叉耦合两个门器件例如反相器来构建一个双稳态逻辑单元,然后这个双稳态逻辑单元选择寄存在两个中的一个状态,就实现了存储一个二进制数字。但是,如果双稳态逻辑单元进入一个不稳定状态,它就可能在不稳定状态之间振荡,但最后会回到双稳态中的一个。而实验表明大多数单元都会有其明确偏向。这个效果是由其对称设计单元参数间的不匹配造成的。而这种不匹配是由制造变化差异引起的,所以能够观察到这样一个存储单元的静态随机存取(Static Random Access Memory, SRAM)单元或一个触发器的稳定状态,就实现了 SRAM PUF^[7,26]和触发器 PUF^[27]。而锁存 PUF^[28]和蝴蝶 PUF^[6]是通过破坏一个单元

之后观察稳定的状态来实现的。所以总结所有的情况,PUF 的激励是一个特定的单元的地址,而响应是单元的稳定状态。

2 PUF 属性

通过第 1 章 PUF 实现方法的归类总结,可以看出 PUF 并不是一个单纯的数学概念,而是嵌入了一些物理实体包含诸多属性有输入输出功能的函数。为了更好地理解 PUF 的基本特性,并在未来的开发工作中能够准确地把握好这些性质,在分析归纳现有 PUF 各种不同定义的基础上总结出 PUF 的 7 个经常出现的属性,并对这些属性进行讨论。

在讨论 PUF 的属性之前,先给出 PUF 的几个相关概念。

定义 1 PUF 是一个物理的激励——响应函数,也就是说,PUF 不是一个纯粹抽象的数学概念。PUF 的输入一般称为激励,用 $x \in X$ 来表示;输出一般称为响应,用 $y \in Y$ 表示。一个激励及其测量的响应一般称为一个激励——响应对,用 $CRP(x, y)$ 表示。描述一个特定 PUF 的激励和响应关系,叫作激励响应对行为 $\Gamma: X \rightarrow Y; \Gamma(x) = y$,其中 Γ 表示物理不可克隆函数。

其次,PUF 的基本应用是实现认证。而在基本的认证过程中会遇到错误认证的情况,人们经常借助片间汉明距离与片内汉明距离这两个概念来描述这个问题。对于一个 PUF,片间汉明距离与片内汉明距离定义如下:

定义 2 片间汉明距离。由于 PUF 的唯一性和不可克隆性会导致两个不同的 PUF 实体产生两个完全不同的响应,所以片间汉明距离是指对两个不同 PUF 实体输入一个特定的激励后,其产生的两个响应之间的距离。

定义 3 片内汉明距离。通常情况下,一个 PUF 响应的精确值不可避免地受到噪声、测量的不确定性和外部因素的影响,所以片内汉明距离是指对一个单一的 PUF 重复两次输入一个特定的激励后,其产生的响应之间的距离。

从上面的描述可以看出,片间汉明距离与片内汉明距离都是测量激励造成的一对响应之间的距离。通常情况下,用直方图来表示一个特定类型的 PUF 的片间汉明距离与片内汉明距离,并且一般用平均值来作为它们的评估指标。这 u_{intra} 表示平均内距离, u_{inter} 表示平均间距离。所以通常期望得到的一个 PUF 的行为是一个尽可能小的 u_{intra} ,而 u_{inter} 尽可能靠近 50%。

下面介绍本文总结归纳的 7 个常见属性。

2.1 鲁棒性

PUF 具有鲁棒性是指当用相同的激励 x 输入 PUF 时,在允许有一小部分错误的条件下,它总是返回相同的响应 $y = \Gamma(x)$ 。这个错误必须在一个很小的考虑距离度量之内。也就是说,这个具有细微差异的响应在距离度量中是非常靠近的。PUF 的鲁棒性主要是通过片内汉明距离直方图来量度并由其实现结果的平均值 u_{intra} 来体现。鲁棒性是 PUF 和伪随机数发生器(Pseudo-Random Number Generator, PRNG)的本质区别属性。在所有已提出的 PUF 实现方法中,几乎所有的 PUF 都具有鲁棒性。

2.2 可计算性

PUF 具有可计算性是指给定 PUF Γ 和激励 x ,可以很容易

地计算出相应的响应 $y = \Gamma(x)$ 。这里的“很容易”可以从不同的角度来解释。从理论的角度来看,它意味着在多项式时间和资源内计算是可行的;而从实际的角度来看,它意味着一个非常低的成本开销,即在有限的时间、空间、功耗和集成芯片的能源等约束条件下,计算是可行的。此外,如果一个 PUF 是可计算的,则表明运行一个 PUF 是可行的。从这个意义上说,所有能提供实验结果的 PUF 实现方法至少在理论上是可计算的。在所有已提出的 PUF 实现方法中,因为光学 PUF 和涂层 PUF 等一些非数字电路 PUF 特殊的构造步骤,所以需要额外的制造步骤或外部测量设备才能满足可计算性。SRAM PUF 需要设备电源才能满足可计算性。而其他大多数 PUF 实现方法都是满足可计算性的,可以说可计算性仅仅是一个实用性的约束。

2.3 唯一性

PUF 具有唯一性是指 PUF 的响应 $\Gamma(x)$ 包含了物理实体嵌入物理不可克隆函数 Γ 的一些身份信息。从信息理论的角度来看,唯一性意味着在 PUF 全体中,一个特定的 PUF 的一些激励响应对(Challenge Response Pair, CRP)满足于唯一标识。也就是说,在理想情况下,一个 PUF 的响应会对全体造成多个分区,这样一来,连续的响应就会使全体的分区越来越小,直到优化了整个分区。这样,CRP 集合就可以唯一认证一个 PUF 的实现。在大多数的实验中,主要是通过片间汉明距离直方图来测量唯一性,并且通过其平均值 u_{inter} 来体现。在已提出的 PUF 实现方法中,所有的 PUF 都具有唯一性。

2.4 不可克隆性

不可克隆性是 PUF 的根本属性,这从“不可克隆”函数的命名上就可以看出。不可克隆性其实是一个程序过程。这个过程可以是物理过程也可以是数学过程,所以不可克隆性可以分为物理不可克隆性和数学不可克隆性。一个 PUF 具有物理不可克隆性是指,给定物理不可克隆函数 Γ ,构造一个物理实体包含另一个物理不可克隆函数 Γ' 使得对于任意 $x \in X$:在很小的错误的情况下 $\Gamma'(x) = \Gamma(x)$ 是困难的。从定义可以看出,物理不可克隆性表示一个对手物理克隆一个 PUF 的困难性。因为产生一个物理克隆的难度甚至可以达到原始物理不可克隆函数 Γ 的制造者也很难实现的程度,所以它也被称为制造者阻力。而一个 PUF 具有数学不可克隆性是指,给定一个物理不可克隆函数 Γ ,构造一个数学程序 f' 使得对于任意 $x \in X$:在很小的错误情况下 $f'(x) = \Gamma(x)$ 是困难的。因为有些实现方法可以容易物理地克隆而不能数学克隆或反之亦然,所以物理和数学不可克隆性是两个根本不同的属性。在所有 PUF 的实现方法中,几乎所有的 PUF 实现方法都具有物理不可克隆性,但数学不可克隆性却很少满足。对于基于仲裁器的 PUF 和一些基于环形振荡器的 PUF 来说,通过使用模型建立攻击很容易破解数学不可克隆性;对于涂层 PUF 和 SRAM PUF 来说,通过搜集很多 CRP 对,也可以容易破解数学不可克隆性。

2.5 不可预测性

PUF 具有不可预测性是指给定一个激励响应对集合 $Q = \{(x_i, y_i(x_i))\} (i = 1, 2, \dots, q)$,很难在一个很小的错误范围内预测响应 $\Gamma(x_c)$,其中 x_c 是一个随机激励且 $(x_c, \Gamma(x_c)) \notin Q$ 。

Q 。在这个定义中可以看出,不可预测性是不可克隆性的松散形式,即不可克隆性意味着不可预测性。在所有 PUF 的实现方法中,大多数 PUF 的实现方法具有不可预测性。对于基于仲裁器的 PUF 和一部分基于环形振荡器的 PUF 来说,通过学习算法可以预测出 PUF 的新的 CRP。也就是说,当对手学习一个 PUF 大量 CRP 时,它就有可能预测出一个新的 CRP,从而消除 PUF 的不可预测性。

2.6 轻量级属性

PUF 具有轻量级属性是指实现物理不可克隆函数 Γ 元器件的数量和大小都是很小的,这在资源有限的设备当中有广泛的应用前景。在如 RFID、传感器网络节点等资源有限的设备当中,一些成熟的加密算法因为器件太多或消耗过大等原因不能使用,所以轻量级就成为硬性的要求^[29-30]。到目前为止,已经提出多种基于 PUF 轻量级的认证计划和密钥生成的应用。在所有 PUF 的实现方法中,数字电路 PUF 更具有这个属性,因为它是利用数字电路内在的变化,而不需要特殊编程实现具体的电路。而且在密钥生成的一些应用中,PUF 的响应不需要存储而是直接传送到电路的输入当中进行下面的计算,这也运用了 PUF 的这个属性。

2.7 防篡改属性

PUF 具有防篡改属性是指当把改变的物理实体嵌入到物理不可克隆函数 Γ' 使得 $\Gamma \rightarrow \Gamma'$ 时,有非常高的概率 $\exists x \in X, \Gamma(x) \neq \Gamma'(x)$ 。从这个定义可以看出防篡改属性是指在篡改发生之后检测篡改攻击的能力。由于 PUF 依赖于微小的物理构造差异,所以人们通常认为篡改一个 PUF 将不可避免地改变 PUF 的激励响应行为。这意味着,对 PUF 的篡改攻击将对 CRP 行为造成不可磨灭的痕迹。在所有 PUF 的实现方法中,只有光学 PUF 和涂层 PUF 是明确防篡改的,其他的 PUF 构造是否具有防篡改属性,还不得而知。

3 PUF 应用

通过前面对 PUF 的实现方法以及基于实现方法提出的属性的描述,得到了 PUF 的一个相对完整的概念。接下来介绍 PUF 的应用,并详细讨论在这些应用中 PUF 的作用和遇到的问题。PUF 主要有四种应用:认证、随机预言机、可计算函数和密钥生成器。

3.1 认证

认证是 PUF 最基本的应用。由于 PUF 的不可克隆、防篡改和轻量级等属性,使用 PUF 用于认证是一种非常有效的防伪技术。所以在 PUF 的相关应用文献中,这是最常见的形式。它的基本原理是:在注册阶段,每一个 PUF 的一些 CRP 连同嵌入 PUF 的物理系统的身份一起被存储在数据库中。在认证阶段,验证者从数据库中挑选一个随机 CRP,然后提供给当前的系统来激励 PUF,如果观察到 PUF 的响应足够接近于数据库中存储的响应,那么认证成功,否则失败。为了防止重放攻击,每个 PUF 的每个 CRP 只能使用一次并且必须在验证结束后从数据库中删除^[31]。

在这样一个过程中会遇到错误认证的问题如图 2 所示。认证错误主要包括两种类型:第一种是错误接受,即通过认证接受了错误的 PUF;第二种是错误拒绝,即通过认证拒绝了正

确的 PUF。一个认证正确与否的阈值分别取决于片内汉明距离直方图和片间汉明距离直方图。如果两个直方图不重叠,就可以通过在两个直方图之间的差距的某处选择阈值来进行无差错的认证,如图 2(a) 所示。但是如果由于设备老化等原因使得它们重叠,那么设置的阈值就必须在错误接受和错误拒绝之间作出权衡,如图 2(b) 所示。从图中可以看出,最佳的选择是通过在两个分布图的交集的某处设置阈值来最大限度地降低错误接受和错误拒绝的总和。但具体的权衡取决于具体的应用。

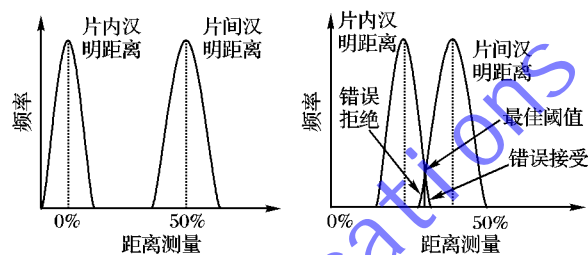


图 2 不同片内和片间汉明距离对认证造成的影响

3.2 随机预言机

随机预言机 (Random Oracle) 是指一个确定性的公共可访问的随机均匀分布函数,对于任意长度的输入,在输出域中均匀选择一个确定性长度的值作为询问的回答。在文献 [32] 中, Bolotnyy 等提出了一个基于 PUF 的方法来提供安全性和隐私保护。它通过使用 PUF 作为一个随机预言机来实现安全性,但是如果没使用随机预言模型的全部属性,那么可能没有必要模拟 PUF 作为一个随机预言机。

3.3 可计算函数

由于基于延迟的数字电路 PUF 可以采用线性不等式来表示,所以它可以用来作为一个可计算函数。这意味着服务器不需要存储 CRP,而是直接计算出预计的响应。这就使得 PUF 具有轻量级的优势,更适合在像 RFID、传感器网络节点等资源有限的设备中使用。但是线性结构带来优势的同时也带来了缺点,即对手很容易通过这个线性结构数学模拟克隆这个 PUF。所以这类 PUF 实现方法的安全性主要面临两个挑战。

第一个挑战是抵抗建模攻击的问题。在一个标准的攻击模型中,对手通过学习了这个 PUF 的一些激励响应以后,给定对手一个新的激励,那么他应该无法预测出相应的响应。在文献 [8] 中, Hammouri 等通过使用线性规划等数学方法,给出了模拟基于仲裁器的 PUF 的一个线性模型。这个线性模型本质是一种激励响应数据库的压缩版本。通过这个线性模型,理论上模拟这个 PUF 可以达到任何级别的精度。为了克服这个问题,在文献 [5, 33-34] 中提出了基于仲裁器 PUF 的非线性变化实现方法,但改进的建模技术^[35]表明这些实现方法也不能幸免于预测。对于基于环形振荡器的 PUF,基于不同的测量方法提出的实现方法^[36]表明它可以安全抵抗模型建立攻击,但这种实现方法和原来的相比有很大的执行开销。

第二个挑战是轻量级的问题,参见第 2.6 节。

3.4 密钥生成器

基于 PUF 的密钥生成在安全领域的应用已经有大量的

文献。如 Tuyls 等^[11]在 Schnorr 的认证协议中使用 PUF,其中用户的密钥被设置为一个 PUF 的响应。同样,Batina 等^[12]使用基于 PUF 的设备密钥来实现 Okamoto 认证协议。

使用 PUF 作为密钥生成器主要考虑使用的是数字电路 PUF。因为在集成电路中,数字电路 PUF 有很好的属性用于密钥生成和存储。通过采用适当的后处理技术,PUF 可用于生产一个加密强密钥,使得方案更具有安全性。由于 PUF 的一些有用属性,使用 PUF 生成密钥有以下优势:

1) PUF 的防篡改属性可以用来提供防篡改的密钥存储。

2) 由于随机性是永久固定在细微芯片的物理构造上,所以不需要传统的非易失性存储步骤。这也额外地提供了对探测攻击和其他可能的侧信道攻击的安全性。PUF 可以在规定的时间内派生出安全密钥并且在使用之后删除,所以密钥不需要永久保存成数字格式,而只是当需要操作时出现在非易失性存储器当中。这就限制了提取设备中密钥的攻击时限。

3) 一个用 PUF 生成的密钥也是密切相关于嵌入 PUF 的物理硬件,使得整个硬件具有物理不可克隆性。

4) 在安全存储一个加密密钥方面,使用具有模糊提取模块的 PUF 比使用非易失性存储单元更有效。

5) 由于密钥生成的数字电路随机性是由不可避免的制造变化引起的,所以不需要明确的密钥编程步骤,这简化了密钥分配。

从 PUF 响应中提取一个安全的密钥需要处理两个主要问题。首先,在不同的测量中,所有数字电路 PUF 实现方法产生的响应都有一个非负概率的错误。因此,在后处理过程中就需要采用一个纠错步骤来保证每次派生出相同的密钥。其次,提取算法需要确保输出的密钥是完全不可预测的,也就是说,它应该是一个均匀分布的随机比特串。由于 PUF 的响应大多数只有部分不可预测,提取算法需要压缩一些响应到一个密钥中以保证强的不可预测性。在文献[37]中,Dodis 等已经研究出同时满足这两个要求的算法,称为模糊提取。模糊提取的主要想法是:在最初的生成阶段,给 PUF 输入一个激励并产生一个响应,然后模糊提取算法根据响应产生一个包含额外信息的密钥。这些额外信息通常被称为辅助数据。这两个都被验证者存储在一个安全的数据库中而不是在设备上。在认证阶段,验证者把辅助数据提供给算法,算法用它来从 PUF 中提取相同的密钥,具体过程如图 3 所示。这样一来,含有 PUF 的设备和验证者之间就建立了一个共享密钥。实际成本实现及其评估可参见文献[38-39]。

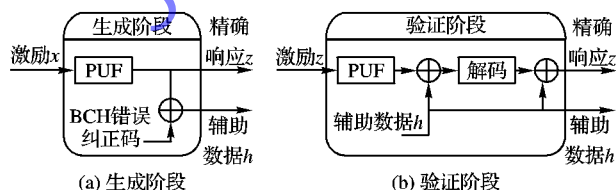


图 3 传统的模糊提取算法

4 未来方向

PUF 领域的相关研究在过去的几年中已经有了很大的进展。无论是在如 RFID、智能卡等资源有限设备中,还是在相对成熟的密码学应用中;无论是在硬件安全领域的认证应用中,还是在软件的密钥生成等算法协议中,PUF 都凭借其具有

不可克隆性、防篡改、轻量级等良好的属性,发挥着不可替代的作用。但是目前在理论探索和应用实践很多方面,PUF 还很不成熟,所以有非常大的研究动力和提升空间。下面简要给出 PUF 研究领域的一些有意义的方向。

在现实安全应用中,PUF 的形式化定义是 PUF 的设计、开发与应用正确性的基础与保证。然而目前提出的 PUF 实现方法的一些形式化定义都或多或少存在各种问题^[35],要么被限制太多,即不包括某些类型的 PUF,要么太虚拟化,甚至假设某些 PUF 的属性。从这个意义上讲,如何给出 PUF 及其属性的严格的形式化定义,仍需要进一步深入的研究。

在过去的几年间,虽然人们提出了大量的 PUF 实现方法,但是通过总结比较发现,这些实现方法的设计都是在孤立的条件下提出的。换句话说,PUF 实现方法的设计都具有临时性。这种情况有些类似于 Shannon^[40]建立扩散和混淆之前的密码设计。那么是否可以提出 PUF 实现方法的系统设计方法,以便人们根据具体的情况来设计实现 PUF,将是一个很有趣的研究方向。

在 RFID 传感器网络节点等资源有限的设备中,基于轻量级属性的 PUF 可以实现大量的应用。但是,前人的工作只是在广泛的意义上提出了 PUF 的轻量级属性,并没有给出 PUF 轻量级属性的具体界限。那么,什么才是 PUF 轻量级属性需求的最低开销?虽然有大量的 PUF 的实现方法和应用,但在这方面却很少有研究。所以使用什么样的理论来考虑、解决这个问题,将是一个全新的研究方向。

5 结语

经过几年的发展,PUF 技术取得了一些进展,但在很多方面还很成熟,所以有非常大的研究动力和提升空间。本文尝试给出目前已经提出的 PUF 技术的一个综述。从本文的讨论中可以知道,PUF 不只是一个简单的概念,而是包括一系列问题的过程函数。本文中主要讨论了 PUF 实现方法、PUF 属性和 PUF 应用,最后对 PUF 的未来研究方向进行了展望。

参考文献:

- [1] GASSEND B, CLARKE D, VANDIJK M, *et al.* Delay-based circuit authentication and applications[C]// ACM Symposium on Applied Computing. New York: ACM, 2003: 294-301.
- [2] PAPPU R S. Physical one-way functions[D]. Boston: Massachusetts Institute of Technology, 2001.
- [3] TUYLS P, SCHRIJEN G J, KORIC B, *et al.* Read-proof hardware from protective coatings[C]// Cryptographic Hardware and Embedded Systems Workshop. New York: ACM, 2006: 369-383.
- [4] LIM D. Extracting secret keys from integrated circuits[D]. Boston: Massachusetts Institute of Technology, 2004.
- [5] LEE JW, LIM D, GASSEND B, *et al.* A technique to build a secret key in integrated circuits for identification and authentication application[C]// Proceedings of the Symposium on VLSI Circuits. Washington, DC: IEEE Computer Society, 2004: 176-159.
- [6] KUMAR S, GUAJARDO J, MAES R, *et al.* The butterfly PUF protecting IP on every FPGA[C]// IEEE International Workshop on Hardware-oriented Security and Trust. Washington, DC: IEEE Computer Society, 2008: 67-70.
- [7] GUAJARDO J, KUMAR SS, SCHRIJEN G J, *et al.* FPGA intrinsic

- PUFs and their use for IP protection[C]// Cryptographic Hardware and Embedded Systems Workshop. Berlin: Springer, 2007: 63 – 80.
- [8] HAMMOURI G, OZTURK E, SUNAR B. A tamper-proof and lightweight authentication scheme[J]. *Pervasive and Mobile Computing*, 2008, 4(6): 807 – 818.
- [9] OZTURK E, HAMMOURI G, SUNAR B. Towards robust low cost authentication for pervasive devices[C]// Proceedings of the Sixth IEEE International Conference on Pervasive Computing and Communication. Washington, DC: IEEE Computer Society, 2008: 170 – 178.
- [10] SADEGHI A R, SCHULZ S, WACHSMANN C. Lightweight remote attestation using physical function[C]// Conference on Wireless Network Security. New York: ACM, 2011: 109 – 114.
- [11] TUYLS P, BATINA L. RFID-tags for anti-counterfeiting[C]// Topics in Cryptology, 2006, LNCS 3860. Berlin: Springer, 2006: 13 – 17.
- [12] BATINA L, GUAJARDO J, KERINS T, *et al.* Public-key cryptography for RFID-tags[C]// Pervasive Computing and Communications Workshops. New York: ACM, 2007: 217 – 222.
- [13] BULENS P, STANDAERT F X, QUISQUATER J J. How to strongly link data and its medium: the paper case[J]. *IET Information Security*, 2010, 4(3): 125 – 136.
- [14] HAMMOURI G, DANA A, SUNAR B. CDs have fingerprints too[C]// Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2009: 348 – 362.
- [15] GUAJARDO J, KORIC B, TUYLS P, *et al.* Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable function[J]. *Information Systems Frontiers*, 2009, 11(1): 19 – 41.
- [16] LOFSTROM K, DAASCH W R, TAYLOR D. IC identification circuit using device mismatch[C]// Proceedings of Solid-State Circuits Conference. Washington, DC: IEEE Computer Society, 2000: 372 – 373.
- [17] HELINSKI R, ACHARYYA D, PLUSQUELLIC J. A physical unclonable function defined using power distribution system equivalent resistance variation[C]// Proceedings of the 46th Annual Design Automation Conference. New York: ACM, 2009: 676 – 681.
- [18] PELGROM M, DUINMAIJER A, WELBERS A. Matching properties of mos transistors[J]. *IEEE Journal of Solid-State Circuits*, 1989, 24(5): 1433 – 1439.
- [19] AGARWAL A, KANG K, BHUNIA S, *et al.* Device-aware yield-centric dual-VT design under parameter variations in nanoscale technologies[J]. *IEEE Transactions on Very Large Scale Integration System*, 2007, 15(6): 660 – 671.
- [20] KANAMOTO T, OGASAHARA Y, NATSUME K, *et al.* Impact of well edge proximity effect on timing[C]// Solid State Circuits Conference, 2007. Washington, DC: IEEE Computer Society, 2007: 115 – 118.
- [21] REDA S, NASSIF SR. Analyzing the impact of process variations on parametric measurements: Novel models and applications[C]// Proceedings of the Conference on Design, Automation and Test. Washington, DC: IEEE Computer Society, 2009: 375 – 380.
- [22] WESTE N. CMOS VLSI design: a circuits and systems perspective[M]. 4th ed. Boston: Pearson Education, 2010.
- [23] GASSEND B, CLARKE D, VANDIJK M, *et al.* Silicon physical random functions[C]// ACM Conference on Computer and Communications Security. New York: ACM, 2002: 148 – 160.
- [24] GASSEND B. Physical random functions[D]. Cambridge, USA: Massachusetts: Massachusetts Institute of Technology, 2003.
- [25] SUZUKI D, SHIMIZU K. The glitch puf: A new delay-PUF architecture exploiting glitch shapes[C]// Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2010: 366 – 382.
- [26] HOLCOMB D E, BURLESON W P, FU K. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags[C]// Proceedings of the Conference on RFID Security. Malaga, Spain: RFID Publications, 2007: 11 – 13.
- [27] MAES R, TUYLS P, VERBAUWHEDE T. Intrinsic PUFs from flip-flops on reconfigurable devices[EB/OL]. [2012 - 03 - 18]. <http://www.cosic.esat.kuleuven.be/publications/article-1173.pdf>.
- [28] SU Y, HOLLEMAN J, OTIS B. A 1.6PJ/bit 96% stable chip-ID generating circuit using process variations[C]// IEEE International Solid-State Circuits Conference. Washington, DC: IEEE Computer Society, 2007: 406 – 611.
- [29] 杨灵, 闫大顺. 基于 PUF 的低成本 RFID 系统安全协议[J]. *计算机工程*, 2010, 36(15): 148 – 150, 155.
- [30] 马昌社, 王涛, 王立斌. 基于 PUF 的 RFID 协议分析与改进[J]. *计算机工程*, 2011, 37(21): 249 – 251.
- [31] MAES R, TUYLS P, VERBAUWHEDE T. Statistical analysis of silicon PUF responses for device identification[EB/OL]. [2012 - 03 - 15]. <http://www.cosic.esat.kuleuven.be/publications/article-1112.pdf>
- [32] BOLOTNYY, L, ROBINS G. Physically unclonable function-based security and privacy in RFID system[C]// IEEE International Conference on Pervasive Computing and Communications. Washington, DC: IEEE Computer Society, 2007: 211 – 220.
- [33] MAJZOBI M, KOUSHANFAR F, POTKONJAK M. Techniques for design and implementation of secure reconfigurable PUFs[J]. *ACM Transactions on Reconfigurable Technology System*, 2009, 2(1): 1 – 33.
- [34] LIM D, LEE J W, GASSEND B, *et al.* Extracting secret keys from integrated circuits[J]. *IEEE Transactions on Very Large Scale Integration System*, 2005, 13(10): 1200 – 1205.
- [35] RUHRAIR U, SOLTER J, SEHNKE F. On the foundations of physical unclonable functions[EB/OL]. [2012 - 03 - 18]. <http://eprint.iacr.org/2009/277.pdf>.
- [36] SUH GE, DEVADAS S. Physical unclonable functions for device authentication and secret key generation[C]// Design Automation Conference. New York: ACM, 2007: 9 – 14.
- [37] DODIS Y, OSTROVSKY R, REYZIN L, *et al.* Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[J]. *SIAM Journal on Computing*, 2008, 38(1): 97 – 139.
- [38] BOSCH C, GUAJARDO J, SADEGHI AR, *et al.* Efficient helper data key extractor on FPGA[C]// Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2008: 181 – 197.
- [39] MAES R, TUYLS P, VERBAUWHEDE T. Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs[C]// Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2009: 332 – 347.
- [40] SHANNON C E. Communication theory of secrecy systems[J]. *Bell Systems Technical Journal*, 1949, 28(4): 656 – 715.