“十三五”科学技术专著丛书

国家自然科学基金青年项目(No.61604020)
湖南省教育厅科学研究项目(No.18B164)

面向安全密钥生成的PUF技术研究与验证

白创 著

Research and Validation of Physical Unclonable Functions for Secure Key Generation Applications

北京邮电大学出版社
www.buptpress.com

“十三五”科学技术专著丛书

国家自然科学基金青年项目(No. 61604020)
湖南省教育厅科学研究项目(No. 18B164)

面向安全密钥生成的PUF技术研究与验证

白　创　著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书针对面向安全密钥生成与存储应用的 PUF 关键技术展开研究与讨论，重点论述增强 PUF 单元工艺敏感性与稳定性的设计方法，提出新型的 PUF 体系结构，设计新的表决机制与扩散算法电路，研究对称布局和等长走线，以及特殊的顶层 S 型网格布线等版图实现技术，最后通过 PUF 芯片的设计仿真测试，说明与验证所研究关键技术的优越性。

本书可作为安全密钥生成、芯片指纹与防伪等硬件信息安全领域的科研人员、工程师，以及高等院校从事信息安全相关专业研究的教师与研究生的参考用书。

图书在版编目(CIP)数据

面向安全密钥生成的 PUF 技术研究与验证 / 白创著. -- 北京：北京邮电大学出版社，2019.2

ISBN 978-7-5635-5663-2

Ⅰ. ①面… Ⅱ. ①白… Ⅲ. ①通信密钥－研究 Ⅳ. ①TN918.4

中国版本图书馆 CIP 数据核字(2018)第 284060 号

书　　名：面向安全密钥生成的 PUF 技术研究与验证

作　　者：白　创

责任编辑：孔　玥

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京九州迅驰传媒文化有限公司

开　　本：787 mm×1 092 mm　1/16

印　　张：8.75

字　　数：185 千字

版　　次：2019 年 2 月第 1 版　2019 年 2 月第 1 次印刷

ISBN 978-7-5635-5663-2　　定　价：39.00 元

前　言

随着芯片攻击技术的发展，存储于ROM等非易失介质中的密钥ID很容易通过版图反向工程和微探测技术等物理攻击方式被截取并且被复制，导致整个加密系统被破坏。物理不可克隆函数(PUF)电路具有良好的安全性和不可克隆性，能够有效地抵御物理攻击且很难被复制，因此它正在逐步地被应用于安全密钥的生成和存储领域。本书以增强唯一性、稳定性和安全性为目标，对面向安全密钥生成和存储应用的PUF关键技术进行了深入的研究。

针对增强稳定性的目标，首先量化计算PUF单元的物理特性，提出利用量化特性对温度和电源电压求导获取相关设计量最优值的增强PUF单元稳定性的方法；然后提出一种新型的PUF体系结构，包括工艺敏感电路、偏差放大电路和偏差比较电路，通过引入偏差放大电路，放大微弱的物理特性偏差，减小其对偏差比较电路的比较精度和各种噪声的敏感性，从而使得比较电路能够产生稳定的输出，提高了PUF的稳定性；最后实现了新型的举手表决机制电路，通过对偏差比较器的输出进行多次采样，按照样本的0/1分布概率判决输出稳定的ID，同时提出采样次数、判决算法和比较阈值三个因素决定举手表决机制生成稳定的ID能力的结论。

针对增强唯一性的目标，首先通过研究器件尺寸和宽长比与器件失配特性之间的关系，提出增强PUF单元工艺敏感性的方法；然后设计了全新的ID扩散算法，保证扩散后的ID在一个大的数值统计空间内满足均匀分布，减小不同ID间碰撞的概率，增强PUF的唯一性。

针对增强安全性的目标，研究了对称布局和等长走线，以及特殊的顶层S型网格布线等版图实现技术。针对版图反向工程的物理攻击方式，研究对称布局和等长走线的版图实现策略，提高PUF的安全性；针对微探测技术的物理攻击方式，提出了顶层S型网格布线方案，有效地抵抗攻击。

基于这些关键技术的研究分析，在0.18 μm CMOS工艺下，最后设计实现四种新型的PUF，包括基于电流饥饿型延迟单元的PUF、基于晶闸管型延迟单元的PUF、基于电阻-二极管型分压单元的PUF和基于纯电阻桥式网络型分压单元的PUF。通过对仿真和测试结果的统计分析比较，分别从唯一性、稳定性和安全性等角度衡量每种PUF的性能。

本书共6章，具体章节组织结构如下。

第1章，绪论。介绍了PUF的基本概念、应用领域和物理特性。在广泛分析国内外相关研究工作的基础上，概括了本书的主要研究内容，并给出本书的组织结构。

第2章，新型PUF单元研究。通过对影响PUF单元工艺敏感性和稳定性的因素分别展开研究，提出了增强PUF单元工艺敏感性和稳定性的设计方法。基于这种方法设计了新型的PUF单元，包括基于电流饥饿型延迟单元、基于晶闸管型延迟单元、基于电阻-二极管型分压单元和基于纯电阻桥式网络型分压电路单元。

第3章，新型PUF电路体系结构研究。提出了新型的PUF体系结构，包括工艺敏感电路、偏差放大电路和偏差比较电路。根据工艺敏感电路的类型，延伸出两类新型PUF电路体系结构，基于延迟单元的PUF电路结构和基于分压单元的PUF电路结构。同时详细阐述了两类PUF电路体系结构各个组成部分的电路结构、版图设计和性能分析。

第4章，PUF性能增强技术研究。针对增强稳定性的指标，提出了高效的举手表决机制的设计方案，并基于方案设计表决电路；针对增强唯一性的目标，实现了一种全新的ID扩散算法，使得扩散后的ID在一个大数值统计空间内满足均匀分布，减小碰撞的概率；针对增强安全性的目标，研究对称布局和等长走线的版图实现策略，以及特殊的顶层S型网格布线技术，有效抵御版图反向工程和微探测技术等物理攻击。

第5章，PUF芯片实现与评测。在0.18μm CMOS工艺下，设计实现了四种新型的PUF，包括基于电流饥饿型延迟单元的PUF、基于晶闸管型延迟单元的PUF、基于电阻-二极管型分压单元的PUF和基于纯电阻桥式网络型分压单元的PUF。通过仿真和测试，综合评估每种PUF的速度、功耗、面积、唯一性、稳定性和安全性等性能。

第6章，结论与展望。对全书研究工作和创新点进行总结，指出未来的研究方向。

由于作者水平有限，加上时间仓促，疏漏甚至错误之处在所难免，不当之处，敬请同行和读者批评指正，联系方式为 baichuang@csust.edu.cn。

作　者

目　录

第 1 章　绪论 …… 1

1.1　PUF 概念与应用 …… 1
1.2　安全密钥生成技术 …… 4
1.3　PUF 物理特性 …… 6
1.4　国内外相关研究工作 …… 7
1.5　本书主要内容 …… 13

第 2 章　新型 PUF 单元研究 …… 15

2.1　PUF 单元工艺敏感性研究 …… 15
2.1.1　器件尺寸与工艺敏感性关系分析 …… 15
2.1.2　器件宽长比 W/L 与工艺敏感性关系分析 …… 16
2.2　PUF 单元稳定性研究 …… 18
2.3　新型 PUF 单元设计 …… 19
2.3.1　延迟型 PUF 单元 …… 20
2.3.2　分压型 PUF 单元 …… 24
2.4　PUF 单元工艺敏感性和稳定性仿真分析 …… 26
2.4.1　延迟型 PUF 单元 …… 27
2.4.2　分压型 PUF 单元 …… 30
2.5　本章小结 …… 33

第 3 章　新型 PUF 电路体系结构研究 …… 35

3.1　新型 PUF 电路体系结构 …… 35
3.2　基于延迟单元的 PUF 电路体系结构 …… 36
3.2.1　基于延迟单元的工艺敏感电路 …… 37
3.2.2　时间偏差放大电路 …… 40
3.2.3　时间偏差比较电路 …… 42
3.3　基于分压单元的 PUF 电路体系结构 …… 43

3.3.1 基于分压单元的工艺敏感电路 …… 43
3.3.2 高增益电压偏差放大电路 …… 44
3.3.3 高精度电压偏差比较电路 …… 45
3.4 本章小结 …… 46

第 4 章 PUF 性能增强技术研究 …… 47

4.1 稳定性增强技术——新型的举手表决机制 …… 47
4.1.1 举手表决机制理论分析 …… 47
4.1.2 举手表决机制电路结构 …… 51
4.1.3 举手表决机制电路实现 …… 56
4.2 唯一性增强技术——全新的 ID 扩散算法 …… 60
4.2.1 扩散算法一 …… 61
4.2.2 扩散算法二 …… 64
4.2.3 扩散算法三 …… 68
4.3 安全性增强技术——特殊的布局布线策略 …… 73
4.3.1 对称布局等长布线技术 …… 73
4.3.2 顶层 S 型网格布线技术 …… 74
4.4 本章小结 …… 76

第 5 章 PUF 芯片实现与评测 …… 78

5.1 基于电流饥饿型延迟单元的 PUF 实现 …… 78
5.1.1 面积、功耗和速度分析 …… 80
5.1.2 唯一性分析 …… 81
5.1.3 稳定性分析 …… 83
5.2 基于晶闸管型延迟单元的 PUF 实现 …… 87
5.2.1 面积、功耗和速度分析 …… 89
5.2.2 唯一性分析 …… 90
5.2.3 稳定性分析 …… 92
5.3 基于电阻-二极管型分压单元的 PUF 实现 …… 96
5.3.1 面积、功耗和速度分析 …… 96
5.3.2 唯一性分析 …… 99
5.3.3 稳定性分析 …… 100
5.4 基于纯电阻桥式网络型分压单元的 PUF 实现 …… 105
5.4.1 面积、功耗和速度分析 …… 105

5.4.2 唯一性分析 …… 108
5.4.3 稳定性分析 …… 109
5.5 四种类型的 PUF 设计性能比较 …… 114
5.6 本章小结 …… 115

第 6 章 总结和展望 …… 117

6.1 总结 …… 117
6.2 展望 …… 119

参考文献 …… 121

第1章 绪 论

近些年来，物理不可克隆函数正逐步广泛地应用于身份认证、密钥生成、指纹识别和防伪技术等安全领域，因此对物理不可克隆函数的研究已经成为当前安全领域的一个研究热点。本书重点研究面向加密系统中安全密钥生成和存储领域的物理不可克隆函数的关键技术。本章首先介绍 PUF 基本概念、应用领域和物理特性，并且通过对传统密钥生成和存储方式局限性的分析，可知面向安全密钥生成应用 PUF 的研究具有重大意义；然后通过对国内外 PUF 研究现状进行分析总结，针对已有 PUF 电路结构的劣势，从增强唯一性、稳定性和安全性的设计目标出发，提出本书的主要研究内容，其中包括：PUF 单元设计、新型的 PUF 体系结构、稳定性增强机制、扩散算法和安全性增强技术等。

1.1 PUF 概念与应用

物理不可克隆函数英文全称是 Physical Unclonable Function(PUF)。PUF 概念最早由 Pappu 于 2001 年 3 月在 *Physical One-Way Functions* 中提出，顾名思义是指系统对应的函数关系是无法克隆与复制的，同时这种函数关系是由某种物理现象的随机特性决定。随后很快就出现了基于光学、电磁学和电子学等原理的多种 PUF 结构，并被广泛地用于信息安全等领域。随着集成电路技术的迅速发展，采用 PUF 技术的集成电路芯片也很快出现，并逐步广泛地应用于身份认证[1-6]、安全密钥生成[7-14]、指纹识别[15-21]和防伪技术[22-23]等领域。PUF 电路主要通过捕获芯片在制造过程中，不可避免产生的器件和连线的工艺偏差，实现将一组输入二进制编码映射为另外一组输出二进制编码的功能。我们将输入的二进制编码定义为激励(challenge)，输出的二进制编码定义为响应(response)，一个激励和响应组成一个激励-响应对(challenge/response pair，CRP)。不同的 PUF 具有不同的 CRP，即使输入相同的激励，不同的 PUF 生成的响应也不同。在某些应用领域中，PUF 产生的一个响应也称为一个 ID。PUF 电路应用方向主要包括身份认证、安全密钥生成、指纹识别和防伪技术四大领域。

1. 身份认证

通过 CRP 进行服务器与安全芯片的认证。每个 PUF 拥有不同的 CRP，出厂前通过测试将不同 PUF 的 CPR 获取并存储于服务器的数据库。当需要进行目标对象认证时，

服务器首先发送一组激励给目标芯片，片上 PUF 根据输入的激励产生对应的响应，并返回给服务器，然后服务器根据发送的激励和接收到的响应查询 CRP 数据库，按照最大匹配方式判断目标芯片是否为合法对象以及是哪一个对象。当需要下一次重新认证或者对不同的目标对象进行认证时，服务器再随机发送一组不同的激励给目标芯片，后续过程是一样的，这样可以有效地抵御重发攻击，保证芯片身份认证的安全性，否则如果每次芯片身份认证过程中，服务器发送的激励都一样，那么攻击者通过多次窃听通信信道上的 CRP，就可以准确地猜测出固定的激励及该目标芯片对应的响应，然后非常容易地复制出具有该固定 CRP 的克隆芯片。随着攻击技术的发展与计算能力的增强，即使在重新对目标芯片进行身份认证时，服务器发送的是随机的与上次不相同的激励，攻击者通过多次读取目标芯片与服务器之间通信信道上的 CRP，然后利用先进的函数拟合算法与高速的数据计算能力，同样可以获得该目标芯片激励与响应之间对应的函数关系，将这种函数关系通过芯片算法实现，就可以冒充原始芯片通过服务器认证，因此这类轻量级 PUF 电路也存在较大的安全风险，需要通过增加 Hash 函数进行安全加固。在目标芯片原有逻辑上增加 Hash 函数，对原始输出的响应进行杂凑散列变换，将变换后的响应发回给服务器完成身份认证，这种方法可以增加通过函数拟合破解目标芯片激励与响应之间对应的函数关系的难度，提高目标芯片身份认证的安全性。

2. 安全密钥生成

PUF 通过捕获芯片制造过程中无法避免的工艺偏差，生成无限多的、具有唯一性和不可克隆性的密钥，这些密钥 ID 不可预测，即使芯片制造商也无法复制，每块加密芯片具有随机的独一无二的密钥 ID，攻击者很难通过软件分析得到，因此极大地提高了加密数据的安全级别。传统加密芯片中的密钥 ID 一般存储于 ROM 等非易失性介质中，通过版图反向工程和微探测技术等物理攻击方式很容易获取非易失介质中的密钥，从而破解整个加密系统，然而基于 PUF 的密钥生成技术，其密钥 ID 由 PUF 通过捕获多称单元的工艺偏差而动态生成，可以有效地抵御版图反向工程和微探测技术等物理攻击，保证密钥 ID 的安全性。这些 ID 比特能够被用作对称密钥，也可以被用作随机种子去生成安全微处理器中的公有/私有密钥对[24]。这类 PUF 目前一般应用于加密处理器、NFC 加密标签等产品中。

3. 指纹识别

通过 PUF 产生用于标识芯片的唯一性 ID，实现对不同芯片的识别。PUF 通过捕获芯片制造过程中的工艺偏差，生成无限多的、不可克隆性的 ID，用于标识不同的芯片，相当于给每一块芯片赋予了一个指纹身份编号。正常工作时，通过读取芯片的指纹身份编号 ID，就可以判断芯片的合法性与具体身份，而实际应用中的芯片身份认证机制考虑的安全性更加复杂，如 RFID 标签的认证机制等，读写器可直接将收到的标签 ID 发送回后台数据库，通过查询数据库认证该标签是否合法及确定标签的身份；而基于随机化 Hash-Lock

协议的RFID认证机制相对复杂，读写器首先发送查询请求，标签收到请求后，计算h(ID+R)，其中ID和R分别为标签的指纹标识和真随机数发生器生成的随机数，h(x)为Hash函数，并将R与h(ID+R)返回给读写器，然后读写器向后台数据库提出需求得到所有标签的ID，接着读写器找寻IDj，满足h(IDj+R)= h(ID+R)，如果发现则标签通过认证，否则认证不成功，并且将IDj发给标签，标签判断是否IDj=ID，如果相等，阅读器通过此次认证，否则认证失败，验证结束。另外还有Hash链协议、基于杂凑的ID变化协议、基于异或运算的超轻量级安全认证协议等都是基于ID的RFID系统安全认证协议，实现均较复杂，但是都离不开原始的ID，而一般RFID标签将ID事先存到ROM等非易失介质中，这种方式储存的ID很容易被窃取导致非法复制标签通过认证，基于PUF的RFID标签认证机制，其ID由PUF动态生成，很难被窃取从而保证RFID标签的合法性得到保障。

4. 防伪技术

通过将PUF集成各类产品包装中，生成用于标识产品唯一性的ID，实现产品的防伪。现有的产品防伪技术包括条形码、二维码、RFID标签等。随着攻击技术的发展，这些防伪技术比较容易被破解与复制，如最常见的二维码防伪技术。一般将二维码印制在正版产品的包装上，打开包装时只要二维码没有被撕毁，就有可能被不法商家回收重新印制在假冒商品上。另外，二维码为由像素构成的图像，通过激光打印很容易打印(复制)出相同的二维码图样，这些二维码图像如被印制到假冒产品上，用户就无法辨别其真伪。而基于PUF的防伪技术很难被破解与复制，由于PUF是通过捕获一致性器件的工艺偏差而生成ID，即使是相同的PUF设计，在生产时每个PUF一致性器件的工艺偏差都不一样，生成的密钥ID也不同，因此很难复制出一样的PUF芯片，或者讲产品包装中PUF具有不可克隆性，另外当产品包装被打开时，PUF电路就遭到破坏，即使假冒产品厂商回收正品包装，也无法还原PUF电路的原始特性，即无法生成与出厂时相同的唯一的ID，这是由PUF电路的固有特性决定的。

针对不同的应用领域，PUF的实现各有特点。面向身份认证的PUF正常工作时需要反馈多组CRP给服务器才能完成认证，并且每次认证过程中接收到的激励都不能重复，另外，在PUF的激励输入和响应输出的部分通常需要增加随机的Hash函数，保证PUF能够抵御模型攻击；面向安全密钥生成的PUF强调生成密钥具有不可克隆性，即使芯片制造商也无法复制，同时强调密钥相对于温度和电源电压变化时稳定性，否则加密系统将无法正常工作，另外强调PUF能够有效地抵御版图方向工程和微探测技术等物理攻击，保证生成密钥无法被截取；面向指纹识别的PUF通过捕获制造工艺的随机偏差，生成无限多的ID，用于标识不同的芯片的身份，其强调产生的ID不可重复，并且每个芯片的ID编号之间的海明距离足够大；面向防伪应用的PUF主要用于甄别商品的真假，同时强调PUF电路的不可还原性，即正品包装被回收重新复原时，原先商品包装打

开时遭到破坏的 PUF 电路也无法还原，无法生成原始的 ID。

综上所述，PUF 电路目前正逐步广泛地应用于身份认证、安全密钥生成、指纹识别和防伪技术等安全领域，而在不同应用领域中，PUF 电路的实现要求也不一样。

1.2 安全密钥生成技术

近些年来，随着互联网技术的快速发展，网络通信数据量呈现爆炸式的增长，人们获取数据信息的方式也越来越便捷高效，然而信息安全问题也变得越来越突出。最常用数据保护方式就是在发送端对数据进行加密处理，然后在接收端对数据进行解密再使用，随着攻击技术的发展，软件加密的方式变得越来越不安全，于是采用硬件实现加密算法（加密芯片）完成对数据的加解密已经成为当前信息安全领域的一个研究热点，硬件加密芯片相比软件加密方式被破解的成本代价更大。通常来说，加密芯片所采用的加密算法是公开的，例如 AES、DES 等对称加密算法，这些算法经过长期验证能够有效地抵御常见的攻击，同时近些年也出现了许多非公开的加密算法，甚至针对相同应用条件下不同用户可以定制不同的加密算法，实现更高级别的安全加密。无论加密算法是否公开，密钥都是私有的，也就是说攻击者即使窃取了加密算法，但是如果没有获取密钥也无法对数据进行解密，因此对于加密芯片而言保证密钥的安全至关重要。早期加密芯片在发送密文时需要同时发送固定密钥，接收端在收到密钥与密文后，采用该密钥结合解密算法对密文解密，这个过程中密钥需要与密文同时发送，或者说密钥完全是裸露在通信信道中，因此攻击者很容易通过窃听方式截取密钥，破坏整个加密系统。后来加密芯片采用随机数作为密钥，随机数一般通过真随机数生成器[25-26]产生，同时定期通过产生新的随机数更新密钥，这样即使密钥被攻击者窃取，由于密钥通过随机数定期更新，也就是说攻击者窃取到的密钥经过一段时间后就失效了，从而提高数据加密的安全性。另外，也出现了 RSA 等非对称公钥加密算法，这类算法的加密所采用的密钥是公开的，接收端在对密文进行解密时采用私有密钥解密，即使加密密钥被截取，由于接收端采用动态私有密钥与非对称解密算法对密文解密才能得到明文，攻击者很难复制原始的动态私有密钥与非对称解密算法种子，故采用 RSA 非对称公钥加密算法的加密数据很难被破解。然而 RSA 加密过程复杂，明文信息量大时整个加密过程时间较长，效率不高，实际加密系统采取 RSA＋AES(DES)结合的方式实现加密，首先利用 RSA 非对称加密算法对密钥进行加密，然后利用 AES(DES)对称加密算法结合密钥对明文进行加密，最后将加密后的密钥与密文发送给接收端，接收端首先利用 RSA 非对称解密算法还原原始密钥，然后利用 AES(DES)对称解密算法结合原始密钥还原密文，但是 RSA 等非对称公钥加密算法数学逻辑复杂，硬件实现开销较大，不适用于低资源开销的芯片应用，同时 AES、DES 等对称加密算法虽然实现逻辑开销相对较小，但是无论固定密钥还是随机数密钥都需要存储于

如 ROM 等非易失介质中，工作过程中在系统时钟[27]驱动下读取密钥实现数据加解密。这种将密钥存储于 ROM 等非易失介质的方式存在三个局限性：

(1) 密钥被写入到 ROM 等非易失介质中，这本身对芯片的制造工艺有特殊要求，传统的数字工艺无法满足要求，需要采用 EEPROM 或者 flash 工艺等，同时 ROM 等非易失介质需要以 IP 核形式购买，一次性付费或者按照芯片数量付费，都增加了芯片的成本开销；如果采用传统的 e-fuse 工艺，还需要在芯片出厂前将密钥通过特殊工艺烧制进 ROM，这同样需要额外的成本。

(2) 密钥存储在 ROM 等非易失介质中，这种方式很不安全，通过版图反向工程和微探测技术等物理攻击方式很容易获取非易失介质中的密钥，从而破解整个加密系统。版图反向工程包括芯片开盖(去封装)、腐蚀覆盖层、磨片去层、化学染色、拍照成像等样片制备的物理过程，然后采用集成电路逻辑分析软件如 ChipLogic 等对各层相片进行电路分析、工艺分析、逻辑提取、版图绘制等步骤实现芯片分析，密钥作为二进制数据存储于 ROM 中，首先对 ROM 结构的各个层次成像，然后一般分析扩散层中电子阴影位置来判断二进制 0/1 数据，从而获取存储于 ROM 中的密钥；微探测物理攻击技术对芯片去封装、覆盖层后，采用 FIB 的方式从顶层开孔至低层的总线信号节点，并且通过填充金属介质将总线信号引到顶层，最后芯片加密工作过程中利用微探针探测读取总线上的密钥值，从而就可以获取密钥。

(3) EEPROM 或者 flash 等非易失介质工艺实现节点较低，如目前主流的 EEPROM 和 Nor flash 工艺节点为 0.18 μm 和 0.13 μm，Nor flash 最先进的工艺节点为 65 nm，而先进的数字工艺可以做到 45 nm、28 nm、10 nm，甚至 7 nm，通过采用先进的工艺可以有效地提高加密芯片包括功能、速度、面积等性能开销，然而 EEPROM 或者 flash 等非易失介质工艺制程升级换代较慢，一定程度上影响了整个加密芯片工艺制程的升级，制约了加密芯片性能的提升；另外 EEPROM 或者 flash 等非易失介质面积开销较大，占据加密芯片总体面积 1/5 至 1/4 是很常见的情况，不利于整个加密芯片面积的缩小。

因此亟需一种成本开销小、实现简单、工艺移植快、安全可靠的密钥生成和存储技术，而物理不可克隆函数(Physical Unclonable Function，PUF)正是这样一种新型的安全密钥生成技术。PUF 电路主要是通过捕获片上相同器件之间的 mismatch 工艺变化特性而生成密钥，电路实现简单，无须特殊制造工艺的支持和额外的成本开销，采用普通工艺即可，工艺移植速度快，并且具有不可克隆性和防止物理攻击特性，能够有效地避免传统密钥生成方法的缺陷，应用于芯片密钥 ID 的生成。

本书主要研究基于 PUF 电路的安全密钥生成关键技术，实现安全密钥的生成，该研究显然具有巨大的现实意义和技术意义。

1.3 PUF 物理特性

面向安全密钥生成的 PUF 电路通过捕获芯片制造过程中产生的器件和连线的随机工艺偏差，生成无限多的密钥 ID，运用于不同的加密芯片实现数据的加解密。PUF 电路一般需要具备四大特性：不可克隆性(unclonable)、唯一性(uniqueness)、稳定性(reliability)和安全性(security)，这些特性是衡量 PUF 设计性能的重要指标。

1. 不可克隆性

不可克隆性是指 PUF 电路生成的密钥 ID 无法预测，一旦一块 PUF 电路出厂，其密钥就确定，即使芯片制造商也无法复制一块完全相同的 PUF 电路。由于 PUF 是通过捕获制造工艺的偏差而生成 ID，不同批次不同 Die，以及相同 Die 上对称单元的工艺偏差是随机的，无法预测，而且这种随机性无法克服，是由工艺制造过程决定的，所以生成的 ID 也不同，事先无法预测。即使一个 PUF 芯片的版图被反向重构，但是在重新制造过程中工艺偏差情况又随机不一样，故新生成的 ID 也不可能与之前的 PUF 完全一致。因此 PUF 芯片具有不可克隆性。

2. 唯一性

唯一性是指 PUF 电路能够产生独立的、不重复的密钥 ID 的能力。具体要求每块 PUF 电路对应的密钥都不相同，即具备唯一的密钥，或者说 PUF 电路生成密钥的重复概率很低，并且每个芯片的密钥之间的海明距离足够大，当环境条件变化时芯片之间密钥碰撞的概率较低。唯一性主要取决于 PUF 对称单元对工艺的敏感性，换句话说取决于 PUF 电路在制造过程中对称单元工艺偏差的大小。PUF 对称单元工艺敏感性越强，对称单元制造工艺偏差越大，PUF 电路的唯一性就越强，也可通过引入独立的唯一性增强机制来改善 PUF 电路的唯一性。而对于其他模块电路则需要减小工艺偏差，实现精准设计，可通过电路设计、工艺优化、设备改善等方式减小工艺偏差。

3. 稳定性

稳定性是指当外界环境条件变化时(温度和电源电压等)，PUF 生成的密钥保持稳定的能力，否则密钥一旦随温度和电源电压等条件变化而改变，整个加密系统就会无法正常工作。稳定性主要取决于 PUF 单元的稳定性，即在温度和电源电压等环境条件变化时，PUF 单元保持输出物理量(延迟时间和分压值等)稳定不变的能力。PUF 输出的物理量偏差随环境条件改变而发生的变化就越小，PUF 单元的稳定性越强，PUF 电路的稳定性也越强，输出密钥 ID 越稳定，也可通过引入独立的稳定性增强机制来改善 PUF 电路的稳定性。

4. 安全性

当 PUF 用于芯片认证时，PUF 每次认证所接收到的激励都不能重复，阻止重复攻击

(replay attack),同时 PUF 需要抵御模型攻击[28-34]等,也要防止攻击者创建软件模型来克隆 PUF 芯片。当 PUF 用于密钥 ID 生成时,安全性是指 PUF 抵抗版图反向工程和微探测技术等物理攻击的能力,保证生成密钥不被攻击者窃取和复制。反向工程通过反向逐层拍照、版图分析获得密钥,微探测技术通过 FIB 打孔灌金属将信号节点引到顶层探测密钥 ID,PUF 设计时需要针对这两种攻击技术的特点,优化 PUF 电路版图布局、布线方式,有效抵御版图反向工程和微探测技术的物理攻击,确保密钥的安全。

总之,不可克隆性、唯一性、稳定性和安全性四大特性是衡量 PUF 设计性能的重要指标,四大特性越好,PUF 的性能也越好。由于 PUF 是利用制造工艺的偏差而生成 ID,每块芯片的工艺偏差是随机的,无法预测,所以生成的 ID 也无法预测。因此即使一个芯片的 ID 被截取,PUF 的版图通过反向工程被重构,但是在重新制造过程中工艺偏差情况不一样,故新生成的 ID 就不可能和截取的 ID 完全一致,所以 PUF 芯片不可能被克隆。同时这种工艺偏差在制造过程中是无法避免的,所以不可克隆性是 PUF 天生具有的特性。因此,本书在 PUF 设计过程中,从唯一性、稳定性和安全性三大特性去衡量 PUF 性能。换句话说,唯一性、稳定性和安全性是 PUF 设计中面临的最重要的三大挑战。

1.4 国内外相关研究工作

近些年来,国内外出现了许多种 PUF 电路结构。根据 PUF 构成单元的不同类型,PUF 主要分为两大类:基于延迟单元的 PUF 电路,其中包括基于判决器的 PUF 电路[35-48]、基于环路振荡器的 PUF 电路[49-60]和基于反相器单元的 PUF 电路[61]等;基于分压单元的 PUF 电路,其中包括基于电源线网格的 PUF 电路[62-64]、基于漏电流的 PUF 电路[65]、基于电流镜单元的 PUF 电路[66]、基于 Butterfly 单元的 PUF 电路[67]、基于 SRAM 单元的 PUF 电路[68-74]、基于 Latch 单元的 PUF 电路[75]和基于敏感放大器单元的 PUF 电路[76]等。下面详细介绍常见的几种 PUF 电路结构和工作原理。

1. 基于判决器的 PUF 电路

基于判决器的 PUF 电路(Arbiter-based PUF)是一种最常见的 PUF 电路,其结构如图 1-1 所示。主要是通过级联多个开关延迟单元(switch delay block)形成两条对称的延迟通路,每一级开关延迟单元包含两个对称的延迟单元,根据选择信号的不同,两个输入信号分别经过不同的延迟单元到达输出,由于芯片制造中对称的延迟单元的工艺偏差不一致,所以级联构成的两条对称的延迟通路延迟时间也不同,多路选择信号组成 PUF 的激励,不同的激励取值导致不同的两条延迟通路;经过两条对称延迟通路后的延迟信号通过由锁存器(latch)或者触发器(filp-flop)构成的判决器(arbiter)判决产生 0/1 的响应,即生成密钥 ID。

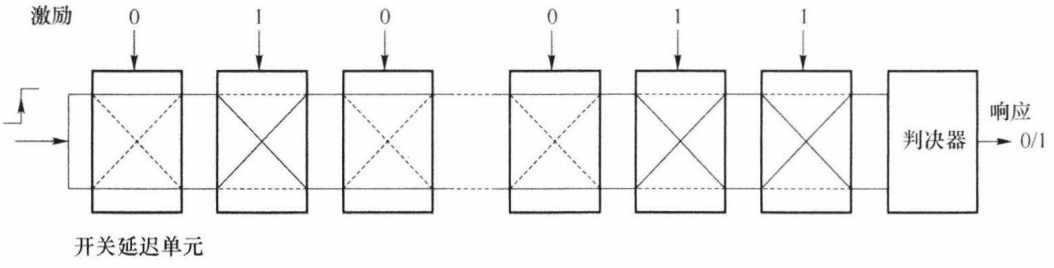

图 1-1　基于判决器的 PUF 电路结构

2. 基于环路振荡器的 PUF 电路振荡器

基于环路振荡器的 PUF 电路(Ring Oscillator-based PUF)是一种基于捕获振荡器(oscillator)频率随工艺变化而产生的微弱变化的 PUF 电路。根据包含振荡器的数量，基于环路振荡器的 PUF 电路的结构分为图 1-2 和图 1-3 两种。按照图 1-2 所示，基于环路振荡器的 PUF 电路由单个可编程振荡器、边沿检测器(edge detector)和计数器(counter)组成，振荡器则由多个一致的负载可编程的延迟单元构成，所有延迟单元的负载编程信号组成 PUF 的激励，边沿检测器用于在固定时间内检测振荡器产生时钟信号的上升沿，计数器则对这些上升沿进行计数，计数结果为 PUF 的响应。由于工艺偏差的存在，每个 PUF 对应的振荡器震荡的时钟频率存在微弱变化，所以输出的响应也不同。

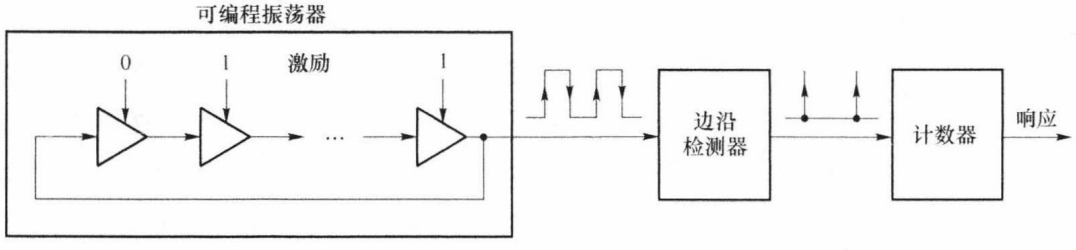

图 1-2　基于单个可编程环路振荡器的 PUF 电路结构

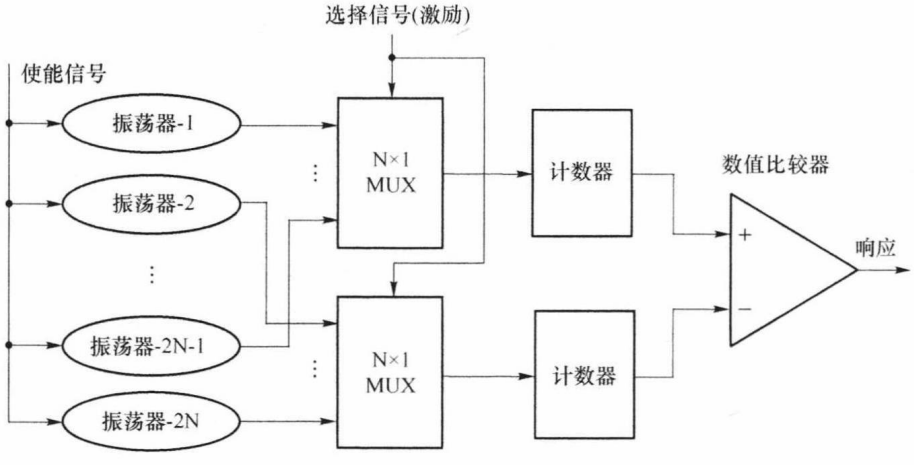

图 1-3　基于 $2N$ 个一致环路振荡器的 PUF 电路结构

而在图 1-3 所示结构中，包含 $2N$ 个设计一致的振荡器、两个 $N\times1$ 多路选择器(Multiplexer)、两个计数器和数值比较器。在制造时由于工艺的偏差，每一个振荡器可以产生具有不同频率的微弱时钟信号，然后根据选择信号的逻辑值，两个 $N\times1$ 多路选择器被用来从 $2N$ 个不同频率的时钟信号中选择两个输出，接着分别通过计数器分别对选出的两路时钟信号进行上升沿计数，最后利用数值比较器对两个计数结果进行比较，判决产生 0/1 输出。这里定义选择信号逻辑值为激励，判决 0/1 输出为响应。

3. 基于电源线网格的 PUF 电路激励

基于电源线网格的 PUF 电路(Power Grid-based PUF)是一种通过捕获对称电源网格电压值随工艺变化而产生的微弱电压差的 PUF 电路。电源布线网格的实现结构如图 1-4 所示。相邻的两层的电源金属线按照垂直角度布线，从而形成网格，交叉点通过通孔连接成为一个 grid，地线按照同样方式布线，电源线 grid 和地线 grid 交错出现。基于电源线网格的 PUF 电路的结构如图 1-5 所示，包含 N 个设计一致的 SMC 和电压比较器。SMC 被部署到芯片的不同位置上，根据扫描数据控制不同的 SMC 轮流工作，在某个时刻，一个或者多个 SMC 可以同时工作。每个 SMC 可以测量所在位置对称网格上电压值，由于对称走线的工艺偏差，所以导致对称网格上的两个电压值存在微弱偏差，同时利用电压比较器对两个电压值进行比较，判决产生 0/1 输出。这里定义扫描数据为激励，判决 0/1 输出为响应。

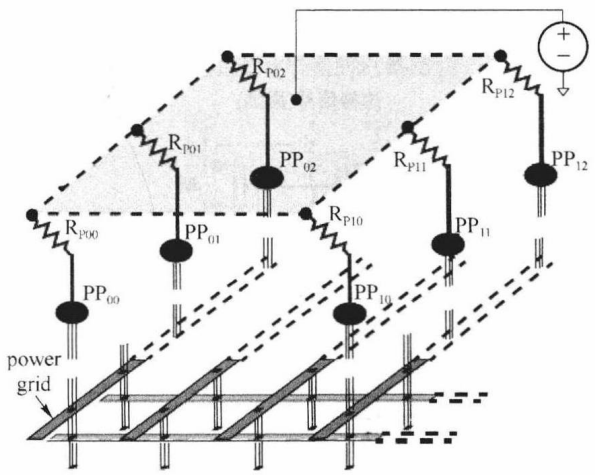

图 1-4 电源线网格的实现结构

4. 基于存储单元的 PUF 电路

基于存储单元的 PUF 电路(Memory-based PUF)是一种基于 memory 单元的 PUF 电路。其整体结构如图 1-6 所示，包含 N 个设计一致的 memory 单元、两个 $N\times1$ 多路选择器(Multiplexer)和电压比较器。memory 单元可以由 SRAM 单元、Latch 单元或 Sense amplifier 单元等实现，其电路结构分别如图 1-7、图 1-8 和图 1-9 所示。显然 memory 单元