稿件编号：JCST-1403-3751

Title：A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs

中文题目：硅物理不可克隆函数综述及基于环形振荡器的物理不可克隆函数研究进展

Abstract: Silicon Physical Unclonable Function (PUF) is a popular hardware security primitive that exploits the intrinsic variation of IC manufacturing process to generate chip-unique information for various security related applications. For example, the PUF information can be used as a chip identifier, a secret key, the seed for a random number generator, or the response to a given challenge. Due to the unpredictability and irreplicability of IC manufacturing variation, silicon PUF has emerged as a promising hardware security primitive and gained a lot of attention over the past few years. In this article, we first give a survey on the current state-of-the-art of silicon PUFs, then analyze known attacks to PUFs and the countermeasures, after that we discuss PUF-based applications, highlight some recent research advances in ring oscillator PUFs, and conclude with some challenges and opportunities in PUF research and applications.

中文摘要:

硅物理不可克隆函数是一种受欢迎的硬件安全原语, 它利用集成

电路制造过程中的固有变化来产生芯片唯一的信息以用于各种安全相关的应用。例如物理不可克隆函数的信息能用于唯一标识芯片，产生秘钥，作为随机数发生器的种子或者给定激励产生对应的响应。由于集成电路制造变化的不可复制和不可预测性，硅物理不可克隆函数已经作为一种迷人的硬件安全原语在过去几年得到广泛的关注。本文首先给出当前硅物理不可克隆函数的研究现状，然后分析针对物理不可克隆函数的攻击及相应的对策，接着讨论基于物理不可克隆函数的应用，然后重点讲述基于环形振荡器的物理不可克隆函数研究进展，最后给出物理不可克隆函数的研究机遇和挑战。

Keywords: Physical Unclonable Function, Hardware security, Trusted IC, VLSI, FPGA

中文关键词：物理不可克隆函数，硬件安全，可信集成电路，超大规模集成电路，现场可编程门阵列