# Protecting Your IP Cores – Part I Soft IP - Foreword

With the surge in globalized hardware design and manufacturing process and rivalry between the IP vendors, threats such as IP piracy/counterfeiting, false claim of ownership are intensifying. As a consequence, the requirements for protection of IP-core designs and the knowhow they epitomize has become of prominence to the industry. As a reusable IP core represents many man-years of design, research and verification testing, a key question is how to protect this investment. It is well acknowledged that the rights of the original IP owner can be abused both deliberately and inadvertently. IP cores, once they are sold by the designer, are hard to keep control on. The main issue here is that once an IP core has been sold, the IP designer has no way of knowing how many times the IP core is actually instantiated. Direct piracy with duplicitous means or reverse engineering may enable direct theft/copying of the IP for re-use without authorization. As a result of counterfeiting the IP, the adversary may even claim the IP to be his own. A system integrator could sell a previously purchased IP core to business associates for a lower price, without the original designer knowing about it. Thus process of nullifying false claims of IP ownership is obligatory.

Over the years, various technologies and strategies have been developed for the protection of IP cores. We will not cover all these technologies in this short presentation. We will also not dive deep into the very details of their working mechanisms and implementations. Instead, we will briefly outline some of the main technologies for soft IP cores only. As to firm and hard IP core, we will leave them to our next parts – Part II and Part III.

In this series of articles, we will divide our talks into several sections as below:

Protecting Your IP Cores – Part I Soft IP, Section One: Encryption Of HDL Codes
Protecting Your IP Cores – Part I Soft IP, Section Two: Watermarking
Protecting Your IP Cores – Part I Soft IP, Section Three: Obfuscation Of Designs
Protecting Your IP Cores – Part I Soft IP, Section Four: Fingerprinting
Protecting Your IP Cores – Part I Soft IP, Section Five: Remote Activation
Protecting Your IP Cores – Part I Soft IP, Section Six: Physical Unclonable Functions(PUFs)
Protecting Your IP Cores – Part I Soft IP, Section Seven: Key-Locking Scheme
Protecting Your IP Cores – Part I Soft IP, Section Eight: Protection Of IP Leakage

Keep in mind that there is no universal and ideal protection valid for all application cases. Most of the time we have to work out an optimal mechanism considering the application scenario as well as cost, time and manpower availability.

## Notes:

This text is part of the book chapter named "*Part 17 IP Core Protection*", which is again part of the book titled

"*Silicon IP – More than just Design*" to be prepared by Mark Chen. You may also find some little more information on the following website http://www.angelia.eu.org/.

保护您的 IP 核——第一部分软 IP——前言

随着全球化硬件设计和制造过程的激增以及 IP 供应商之间的竞争，IP 盗版/假冒、虚假所有权等威胁正在加剧。因此，保护 IP 核设计的要求及其代表的专有技术已成为业界的重点。由于可重复使用的 IP 核代表了多年的设计、研究和验证测试，因此一个关键问题是如何保护这项投资。众所周知，原知识产权所有者的权利可能被有意或无意地滥用。 IP 内核一旦被设计人员出售，就很难控制。这里的主要问题是，一旦 IP 核售出，IP 设计人员就无法知道 IP 核实际实例化了多少次。采用双重手段或逆向工程的直接盗版可能导致直接盗窃/复制 IP 以在未经授权的情况下重复使用。由于伪造 IP，攻击者甚至可能声称 IP 是他自己的。系统集成商可以以较低的价格将先前购买的 IP 核出售给业务伙伴，而原始设计人员并不知道。因此，取消知识产权所有权的虚假声明的过程是强制性的。

多年来，为保护 IP 内核开发了各种技术和策略。在这个简短的介绍中，我们不会涵盖所有这些技术。我们也不会深入研究它们的工作机制和实现的细节。相反，我们将简要概述一些仅用于软 IP 内核的主要技术。至于固件和硬核 IP，我们将把它们留给我们的下一部分——第二部分和第三部分。

在本系列文章中，我们将把我们的谈话分为以下几个部分：

保护您的 IP 内核——第一部分软 IP，第一节：HDL 代码的加密
保护您的 IP 内核 – 第 I 部分软 IP，第二部分：水印
保护您的 IP 内核——第一部分软 IP，第三部分：设计的混淆
保护您的 IP 内核 – 第 I 部分软 IP，第四部分：指纹识别
保护您的 IP 核 – 第 I 部分软 IP，第五部分：远程激活
保护您的 IP 内核 – 第 I 部分软 IP，第 6 节：物理不可克隆函数 (PUF)
保护您的 IP 核 – 第 I 部分软 IP，第 7 节：密钥锁定方案
保护您的 IP 内核 – 第 I 部分软 IP，第 8 节：保护 IP 泄漏

请记住，没有适用于所有应用案例的通用且理想的保护。大多数时候，我们必须考虑应用场景以及成本、时间和人力可用性来制定最佳机制。

说明：

本文是"第 17 部分 IP 核保护"一书章节的一部分，该章节也是由 Mark Chen 编写的"硅 IP – 不仅仅是设计"一书的一部分。您还可以在以下网站 上找到更多信息。