# SILICON IP – MORE THAN JUST DESIGN

## VOLUME 17: IP CORE PROTECTION – Part IV General IP - Chapter IV-03 Remote Activation

In order to prevent illegal copying, a designer must be able to know how many times a particular IP core has been instantiated. Moreover, by allowing the designer to remotely activate an IP core, pay-per-use licensing would be possible. Finally, with remote activation comes pre-activation mode. If this mode is degraded, illegal copies can be effectively made useless until they are properly activated by the original IP designer. Obviously, such a remote activation scheme should also be secure, so that ill-intentioned users cannot circumvent it and use an illegal copy of the IP core.

### PUF (Physical Unclonable Function) Based Remote Activation

The PUF Based Remote Activation aims at providing IP core designers with a secure remote activation system for IP cores.

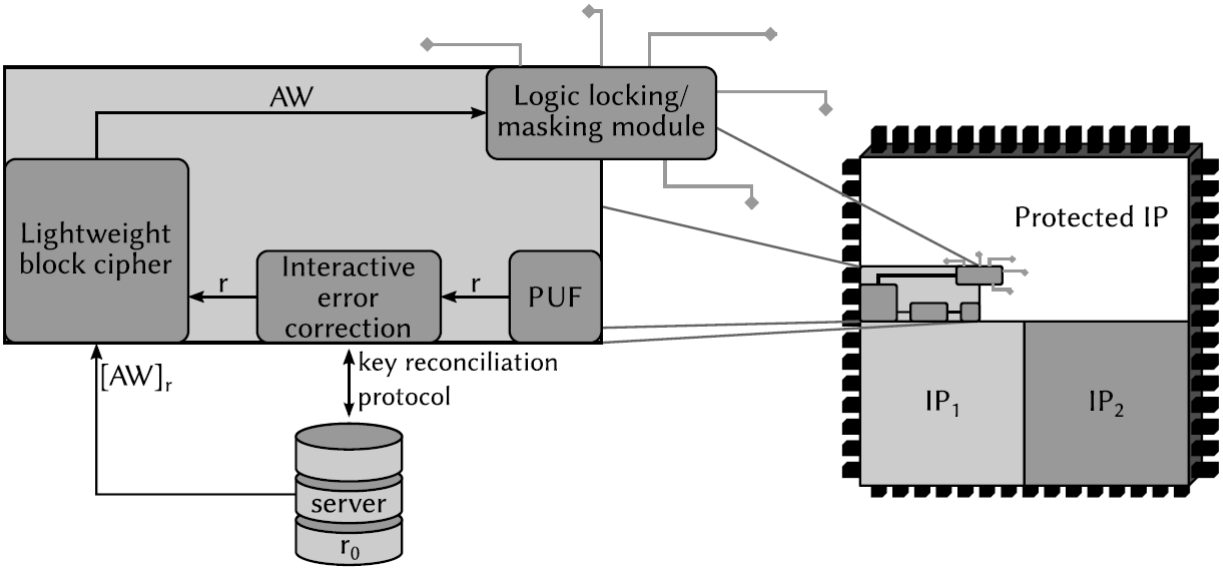
An overview of the IP protection module is shown in figure below. On the right-hand side, an integrated circuit that integrates three IP cores is shown. One of them is protected by the module detailed on the left-hand side, which communicates with a remote server shown at the bottom. This module comprises the following components:

**Lightweight block cipher**
It decrypts the encrypted activation word sent by the remote server. The encryption key is the PUF response.

**Logic locking/masking module**
It locks or masks the protected IP core and makes it unusable when not activated yet.

**PUF**
It generates a unique identifier for the IP core instance.

**Interactive error correction**
It makes the device-side and server-side responses (r and r0) match by carrying out a key reconciliation protocol.




Overview of the IP protection module

VOLUME 17 IP CORE PROTECTION – Part IV General IP - Chapter IV -03 Remote Activation Overview of the IP protection module

**REMOTE ACTIVATION OF ICS FOR PIRACY PREVENTION AND DIGITAL RIGHT MANAGEMENT**

The researchers introduced a remote activation scheme that aims to protect integrated circuits (IC) intellectual property (IP) against piracy. Their remote activation enables designers to lock each working IC and to then remotely enable it. The new method exploits inherent unclonable variability in modern manufacturing for unique identification (ID) and integrate the IDs into the circuit functionality. The objectives are realized by replication of a few states of the finite state machine (FSM) and adding control to the state transitions. On each chip, the added control signals are a function of the unique IDs and are thus unclonable. On standard benchmark circuits, the experimental results show that the novel activation method is stable, unclonable, attack-resilient, while having a low overhead and a unique key for each IC.