SILICON IP – MORE THAN JUST DESIGN

VOLUME 17: IP CORE PROTECTION – Part IV General IP - Chapter IV-04 Active IP Control

ACTIVE CONTROL FOR IP CORE PROTECTION

A new approach is presented that can actively control multiple hardware intellectual property (IP) cores used in an integrated circuit (IC). The IP rights owner(s) can remotely monitor, control, enable, or disable each individual IP on each chip. The IPs can be controlled by the original designer or by the designers who reuse them. Each IP has a built-in functional lock that pertains to the unique unclonable ID of the chip. A control structure that coordinates the locking and unlocking of the IPs is embedded within the IC. A trusted third party approach is introduced for issuing certificates of authenticity, in case it is required for the applications.

Figure 1 presents a reuser's design which contains multiple IP cores. The cores denoted by IP1, IP2, : : : , to IPK are the protected ones. The functional control unit of each IP is represented by a finite state machine (FSM). The circuit designers (reusers) include two new modules in their designs. One added part is an identification (ID) circuitry that extracts the unique identification bits for the chip using the silicon variability. The other addition is a control module that is embedded within the central controller of the chip. Each protected IP is directly connected to the ID circuitry. Each of the protected IPs contains a lock within their functional states.

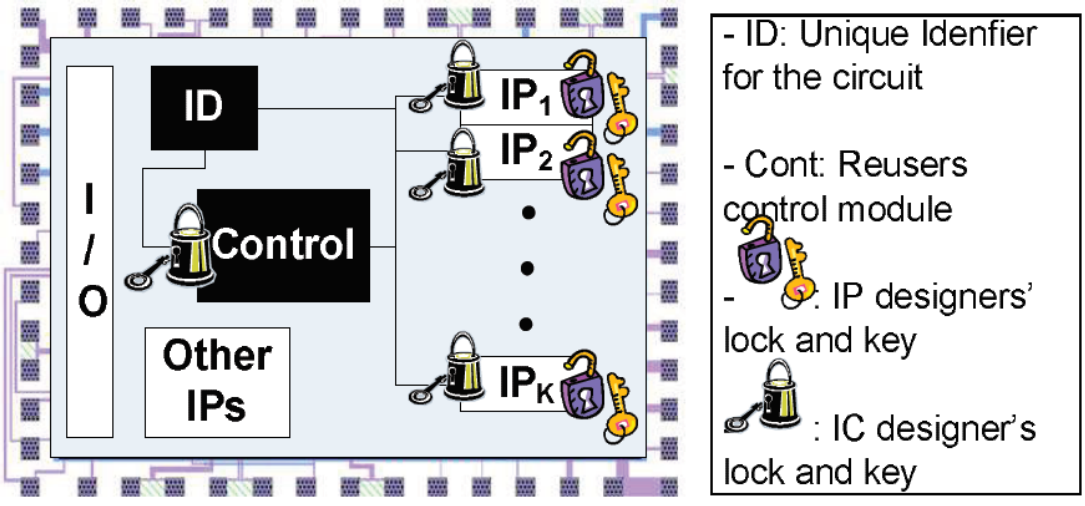

Fig 1 A reuser's design including multiple IP cores. Each IP may be locked/unlocked by the IP designer or the reuser, depending on the application

The remote enabling/disabling provides two sets of locks and keys, one for the designer and one for the reuser. The locks are embedded within the control structure of each IP that can be represented by a finite state machine

(FSM). There are two major advantages for the selected locking/unlocking mechanism:

(i) the IDs come from the verifications of the physical structure of silicon and are therefore random and unclonable, and

(ii) the locks are integrated within the functional control structure, so removing or tampering the lock would tamper the functionality, rendering the IP unusable. Furthermore, as we will show, modifying the FSM does not result in a significant overhead.

Many protection, security, and DRM protocols can be enabled by the new IP locking/unlocking method. For example, the core providers can protect their IPs against over-building a licensed product, since each IP would be locked upon manufacturing. As another example, the reuser who has another set of locks/keys on the IP can select which IPs (or even features) are activated on the chip, e.g., for charging the customers who are willing to pay for added features.

FLOW OF THE ACTIVE CONTROL FOR IP CORES

Figure 2 shows the overall flow of the new IP protection approach. There are four main entities involved:

(i) IP rights owners (IP designers) who design, format and sell the individual IPs,

(ii) IC rights owner (reuser) who integrates multiple IPs, including the open IPs and I/O interfaces, into one IC,

(iii) The fabrication plant (fab), and

(iv) an authorized system verifier; called certificate authority (CA). This entity ensures the trust between hardware IP providers, reusers, and the fab.

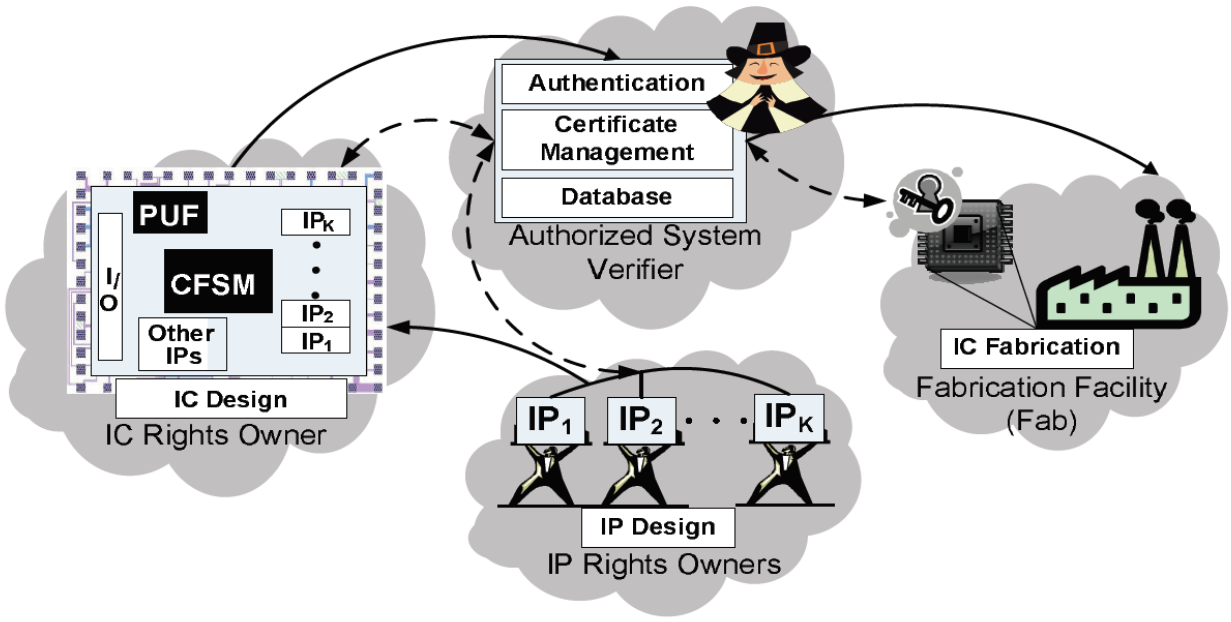

Figure 2 flow of IP active control

The flow can be described as follows.

The IP designer forms the FSM of the design by using the high level design description. Then, the lock(s) are strategically embedded in the FSM. The modified finite state machine is called the boosted finite state machine (BFSM). The reusers may integrate multiple locked IPs, in addition to other components, including their own designs, unlocked IPs, I/O peripherals, memory, and the master identification/control parts. The master

identification/control consists of a controlling finite state machine (CFSM) and a PUF (physically unclonable functions). The CFSM interacts and controls the various IPs; it can enable/disable the other components. The PUF provides a mean for identifying each IC implementing the design in a unique and unclonable way.

The ready-to-fab designs are shipped to the CA who certifies the IP cores and the reuser. The material is then sent to the fab who makes the masks and produces a number of ICs as specified by the contract. The operations described so far are shown by solid arrows on the figure. The dashed arrows present the steps required for key exchange transactions.

The fabricated ICs are nonfunctional and have locks on the CFSM and on the protected IPs from the providers. For each IC, the fab tests the PUF input and runs it through the IP flip flops (FFs) scan chain. The state of the IC will be read out from the FFs and sent to the CA who will in turn supply the state of each chip to the authorized reusers and IP providers. Each of the contacted parties will produce the specific keys to unlock the component. Also, the IP provider computes the error correcting code (ECC) for the lock, to mask the possible few changes caused by the fluctuations in the PUF identifiers. The keys are then sent back to the CA, who certifies the consent of the rights owners before sending them to the fab.