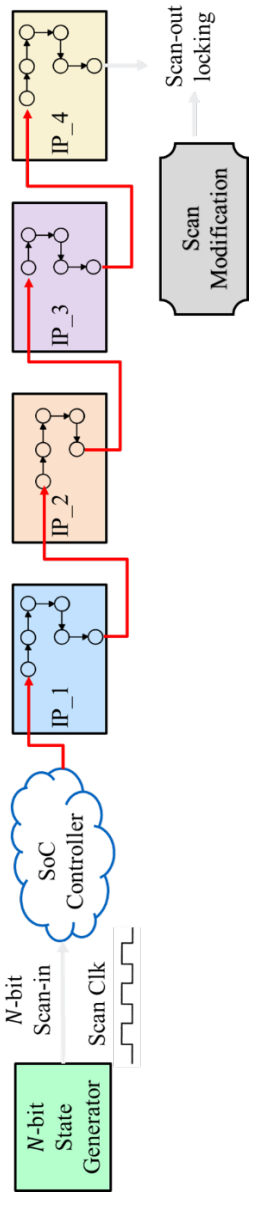
Caspia Technologies
End-to-End Security Solutions for Electronics Supply Chain

FASLock: Functional and Scan Logic Locking

Caspia Technologies

http://caspiatechnologies.com/

The rapid shrinking of the time-to-market and the increased complexity of developing integrated circuits have forced design houses to rely on untrusted third parties to access various intellectual properties (IPs), perform design integration, and fabricate/package chips. This horizontal shift in the new business model has introduced the risk of IP piracy, tampering, reverse engineering, counterfeiting, and overproduction. Different protection techniques have been introduced to mitigate these problems. Among them, logic locking has emerged as the most promising solution.



Logic locking is based on adding keys to the design to hide the original functionality and prevent reverse engineering, overproduction, and tampering. The design will be unlocked and functional when the correct key is loaded from the tamper-proof memory. However, it has been shown that boolean satisfiability (SAT)-based attacks, physical attacks, as well as, machine learning attacks can successfully extract the (secret) locking keys since the design is statically locked using the existing solutions. Moreover, most of these techniques are ad-hoc and not-based on mathematical and formal proofs. For example, the existing techniques may consider inserting key gates to result in high output corruptibility. However, it has been shown that maximizing the output corruptibility will increase the chance of SAT-based attacks to retrieve the locking keys. Furthermore, most of these techniques consider locking the functional parts of the design, while debugging and testing infrastructures are remained unprotected, and they can be utilized to make SAT attacks successful, by increasing the design observability. Therefore, it is essential to develop effective and resilient logic locking techniques to simultaneously protect both the functional and testing infrastructures against the aforementioned attacks.

Caspia Technologies
End-to-End Security Solutions for Electronics Supply Chain

Caspia Technologies' solution, FASLock, is a dynamic approach that can effectively lock both functional components and scan infrastructure of the design. FASLock dynamically hampers the correct transition of the design's finite state machines, which eventually leads to the corruption of the overall functionality. The same technique can be used to obfuscate the scan patterns to block the possibility of SAT attacks. FASLock is provable secure and blocks SAT-attacks, machine-learning, and physical attacks.

Combining scan locking and functional locking will drastically decrease the area and power overhead. While its area overhead is extremely small, it is mathematically strong and comparable to advanced encryption’s strength. FASLock is augmented with formal proofs that the technology increases the locking protection's strength toward SAT and machine learning based attacks by several orders of magnitude.