A generally held opinion in the industry is that scan technology carries the potential of being misused to access proprietary design information, presenting a security risk to the semiconductor vendor’s intellectual property (IP). For example, scan access can be used to learn something about the number of flip-flops in a design, which in turn indicates information about the performance-related blocks in the design. Scan access can also be used for fraud, where critical information is stored on the chip.

Can we do without scan when security is an issue? ATPG for any reasonably sized design relies on scan circuitry to create a test set with high fault coverage. Scan technology removes sequentiality from the design that allows for test generation algorithms to successfully find tests for the targeted faults. Sequential ATPG technology has not made enough progress to be deployed for the testing of any large sequential design in the industry. Thus, scan is an uncompromised requirement for high-quality testing.

Given that scan test is needed, one has to be sensitive to the concerns that scan technology provides controllability and observability in the IC, which could ease IP theft. While there is no documented history of scan technology being used in this manner, the potential of its misuse exists.

However, the solution is not to eliminate scan chains, but to add security to design-for-test (DFT) as a design constraint.

Consider the scan design in Figure 1. It would be a relatively simple task to key-code encrypt the design to include decoding logic between the scan-in and the scan chains, and encoding logic between the scan chains and the scan-out (such that the decoding logic is not the inverse of the encoding logic). Once encrypted, a user knowing how to operate the scan chains may store and extract values from internal flip-flops of the design, but would need to have the decryption/encryption details to actually operate the scan chains.

Currently, the test industry uses test logic (DFT) similar to that shown in Figure 1. Test compression technology today, which enables the reduction of test data volume and test application time, can be readily modified to prevent the extraction and reverse-engineering of a design’s IP.

Conclusions
Scan chains with decryption and encryption technology allow for scan chains to be used in security sensitive situations. Scan chains (and hence high-quality test) can be implemented on ICs without compromising the IP on the chip.