Embedded systems such as smart card or IoT devices should be protected from side-channel analysis (SCA) attacks.  For the secure hardware implementation, SCA security metrics to quantify robustness of the implementation at the abstraction level from the logic level to the layout level against SCA attacks should be considered. In our design flow, the first security test is executed at the logic level. If the implementation does not satisfy the threshold of the SCA security metric based on Kullback-Leibler divergence,  the module can be re-synthesized with secure logic styles such as WDDL or *t-*private logic circuits.  At the final security test, we use the machine learning technique such as LDA, QDA, SVM and naive Bayes to check the distinguishability of the side-channel leakage depending on inputs or outputs. These techniques apply to an ASIC in characterizing the secret data leakage.

 In this thesis, *t*-private logic circuits are implemented with the FreePDK45nm.  The SCA security metric as well as the delay and power consumption is characterized. All this characterization data are stored in the standard liberty format(.lib) in order for general CAD tools to use this file. The *t*-private logic package including  the general digital logics can be exploited for secure VLSI design. Also, various classifiers such as LDA, QDA, SVM and naive Bayes are used to emulate real SCA environment. Based on this SCA simulator, the threshold of the SCA security metric can be estimated and the security can be verified more accurately. The secure logic cell package and SCA simulator support the methodology of the secure hardware implementation.