HArdware Trojan vulnerability

**Abstract**

Many basic analog blocks and structures, which contain positive feedback loops, are vulnerable to the presence of one or more undesired stable equilibrium points. The phenomena of multiple equilibrium points is investigated with emphasis on using a temperature-domain representation to identify equilibrium points in some circuits that have a single positive feedback loop. It is shown by example that the presence of multiple equilibrium points can often be observed as hysteresis in a plot of an output circuit variable versus temperature obtained from a bidirectional temperature sweep over a temperature interval [$T\_{1},T\_{2}$] of interest. The hysteresis can be associated with a relationship comprised of a single continuous locus of points or comprised of two or more disjoint continuous loci of points. Any continuous locus of points in this relationship that does not include either of the temperature interval endpoints [$T\_{1},T\_{2}$] will be termed an “isolation region”. Challenges of determining the presence or absence of multiple stable equilibrium points with standard approaches to simulation and mixed-signal verification will be discussed. Vulnerability of circuits to analog hardware Trojans where the location and size of the hysteresis window can be engineered to serve as a Trojan trigger will be addressed. Concern associated with exploitation of an isolation region as a method for embedding and triggering analog hardware Trojans that are extremely difficult to detect will be raised.

Keywords— Positive Feedback Loop; Hardware Trojan; Isolation Region; Inverse Widlar circuit; Wilson circuit