Production of Integrated Circuits (ICs) has been largely strengthened by Globalization. System-on-chip providers are capable of utilizing many different providers which can be responsible for a single task. This Horizontal structure drastically improves to time-to-market and reduces manufacturing cost. However, untrust of oversea foundries threatens to dismantle the complex economic model currently in place. Many Intellectual Property (IP) consumers become concerned over what potential malicious or unspecified logic might reside within their application. This logic which is inserted with the intention of causing harm to a consumer has been referred to as a Hardware Trojan (HT).

To help IP consumers, researchers have looked into methods for finding HTs. Such methods tend to rely on high-level information relating to the circuit, which might not be accessible. There is a high possibility that IP is delivered in the gate or layout level. Some services and image processing methods can be leveraged to convert layout level information to gate-level, but such formats are incompatible with detection schemes that require hardware description language. By leveraging standard graph and dynamic programming algorithms a set of tools is developed that can help bridge the gap between gate-level netlist access and HT detection. To help in this endeavor this dissertation focus on several problems associated with reverse engineering ICs. Logic signal identification is used to find malicious signals, and logic desynthesis is used to extract high level details.

Each of the proposed method have their results analyzed for accuracy and runtime. It is found that method for finding logic tends to be the most difficult task, in part due to the degree of heuristic's inaccuracy. With minor improvements moderate sized ICs could have their high-level function recovered within minutes, which would allow for a trained eye or automated methods to more easily detect discrepancies within a circuit's