Due to the globalization of integrated circuit (IC) design in the semiconductor industry and outsourcing of chip manufacturing, third-party intellectual properties (3PIPs) become vulnerable to IP piracy, reverse engineering, counterfeit IC, and hardware Trojans. To thwart such attacks, ICs can be protected using logic encryption techniques. However, strong resilient techniques incur significant overheads. Side-channel analysis attacks (SCAs) further complicate matters by introducing potential attacks post-fabrication. One of the most severe SCAs is power analysis (PA) attacks, in which an attacker can observe the power variations of the device and analyze them to extract the secret key. PA attacks can be mitigated via adding large extra hardware; however, the overheads of such solutions can render them impractical, especially when there are power and area constraints. In our first approach, we present two techniques to prevent normal attacks. The first one is based on inserting multiplexers equal to half/full of the output bit number. In the second technique, we first design polymorphic logic gates (PLGs) using silicon nanowire field-effect transistors (SiNW FETs) and then replace some logic gates in the original design with their SiNW FETs-based PLGs counterparts. In our second approach, we use SiNW FETs to produce obfuscated ICs that are resistant to advanced reverse engineering attacks. Our method is based on designing a small block, whose output is untraceable, namely untraceable resilient SAT (URSAT). Since URSAT may not offer very strong resilience against the combined approximate SAT-removal attack, S-URSAT is achieved using only CMOS-logic gates, and this increases the security level of the design to robustly thwart all existing attacks. In our third topic, we present the usage of all spin logic devices (ASLDs) to produce secure and resilient circuits that withstand IC attacks (during the fabrication) and PA attacks (after the fabrication). We show that ASLD has unique features that can be used to prevent PA and IC attacks. In all of our three topics, we evaluate each design based on performance overheads and security guarantees.