The emergence of hardware Trojans has largely reshaped the traditional view that the hardware layer can be blindly trusted. Hardware Trojans, which are often in the form of maliciously inserted circuitry, may impact the original design by data leakage or circuit malfunction. Hardware counterfeiting and IP piracy are another two serious issues costing the US economy more than $200 billion annually. A large amount of research and experimentation has been carried out on the design of these primitives based on the currently prevailing CMOS technology.

However, the security provided by these primitives comes at the cost of large overheads mostly in terms of area and power consumption. The development of emerging technologies provides hardware security researchers with opportunities to utilize some of the otherwise unusable properties of emerging technologies in security applications. In this dissertation, we will include the security consideration in the overall performance measurements to fully compare the emerging devices with CMOS technology.

The first approach is to leverage two emerging devices (Silicon NanoWire and Graphene SymFET) for hardware security applications. Experimental results indicate that emerging device based solutions can provide high level circuit protection with relatively lower performance overhead compared to conventional CMOS counterpart. The second topic is to construct an energy-efficient DPA-resilient block cipher with ultra low-power Tunnel FET. Current-mode logic is adopted as a circuit-level solution to countermeasure differential power analysis attack, which is mostly used in the cryptographic system. The third investigation targets on potential security vulnerability of foundry insider's attack. Split manufacturing is adopted for the protection on radio-frequency (RF) circuit design.