Abstract

Hardware security is essential to the prevention of cloning, theft of service and tampering. Effective hardware security starts with secure key storage. The level of security provided by a key is dependent upon the effort an attacker needs to expend to compromise the key. The sophistication of the tools that are used to carry out such attacks has increased significantly over the years, compromising the protection of traditional key-storage approaches. A radically new approach is needed to counter this increased threat. Rather than trying harder to conceal the key in the hardware, a revolutionary approach has emerged in which the key is simply not stored. This new approach to hardware security relies on the unique electronic "fingerprint" inherent in every semiconductor device and is known as Hardware Intrinsic Security (HIS).