Abstract
As tooling charges for ASICs increase inexorably over time, FPGAs become the technology of choice for a wider variety of applications. Today many designers are implementing secure systems using FPGAs and the shift towards FPGA can be expected to accelerate. Although FPGA chips are compelling from a cost and ease of use perspective they also have a unique set of security challenges, quite different from those faced on ASIC chips. Moreover, many of the established countermeasure techniques used on ASIC chips are not available to the FPGA designer working.

This talk will consider the threat model for designers using FPGA. The two most important challenges are protecting the intellectual property in the user design against reverse engineering and cloning and, for designs which implement a security function, hardening the design against tampering and side channel attacks. Unfortunately, many of the most popular commercial FPGA families have not been designed with security in mind which limits the level of security that is achievable.

This talk will consider the various technical mechanisms which have been proposed to address these challenges, outline their strengths and weaknesses and provide guidance on how to obtain reasonable levels of security in real world applications.