Physical Unclonable Functions and Secure Processors

Srini Devadas

Professor and Associate Head
Department of EECS, MIT, Cambridge

Abstract

As computing devices become ever more pervasive, two contradictory trends are appearing. On one hand computing elements are becoming small, disseminated and unsupervised. On the other hand, the cost of security breaches is increasing as we place more responsibility on the devices that surround us. The result of these trends is that physical attacks present an increasing risk that must be dealt with.

Physical Unclonable Functions (PUFs) are a tamper resistant way of establishing shared secrets with a physical device. They rely on the inevitable manufacturing variations between devices to produce an identity for a device. This identity is unclonable, and in some cases is even manufacturer resistant (i.e., it is impossible to produce devices that have the same identity).

We describe a few applications of PUFs, including authentication of individual integrated circuits such as FPGAs and RFIDs, and the production of certificates that guarantee that a particular piece of software was executed on a trusted chip.

We present the design and implementation of two PUF-enabled devices that have been built: a low-cost secure RFID that can be used in anti-counterfeiting and other authentication applications, and a secure processor capable of performing certified execution and higher-level cryptographic functions.

The PUF-enabled RFID uses a simple challenge-response protocol for authentication that shifts complexity to the reader or server and therefore only requires a small number of transistors on the device side. The PUF-enabled processor generates its public/private key pair on power-up so its private key is never left exposed in (on-chip or off-chip) non-volatile storage. It is capable of a broad range of cryptographic functionality, including certified execution of programs.