On the Possibility of Cryptography without (so many) Secrets

Shafi Goldwasser

Abstract

The absolute privacy of the secret-keys associated with cryptographic algorithms has been the corner-stone of modern cryptography. Still, in practice, keys do get compromised at times for a variety or reasons. A particularly disturbing loss of secrecy is as a result of side channel attacks. These attacks exploit the fact that every cryptographic algorithm is ultimately implemented on a physical device and such implementations enable 'observations' which can be made and measured on secret data and secret keys. Indeed, side channel observations can lead to information leakage about secret keys. Traditionally, such attacks have been followed by ad-hoc 'fixes' which make particular implementation invulnerable to particular attacks, only to potentially be broken anew by new examples of side-channel attacks.

In recent years, several theories of how to achieve provable security against a large class of families of side channel attacks have been proposed. Examples of such families include (1) the `computation but only computation' (of Micali and Reyzin) attacks where one assumes that computation proceeds in steps and the only portions of secret memory which may leak during a computational step are those which effect its outcome, and (2) the `Memory-attacks' proposed (of Akavia, Goldwasser, and Vaikuntanathan) that assumes that any function of the entire secret memory may leak as long as its output is of bounded length.

Provably secure cryptographic constructions, under standard cryptographic intractability, have been proposed for the above attack models. These include constructions of encryption scheme, digital signatures schemes, pseudo random number generators, and even general computations under the additional assumption of the existence of simple secure hardware (one-time memory).

The talk will survey highlights of these developments.