New Developments in Leakage-Resilient Cryptography

Vinod Vaikuntanathan

Microsoft Research
vinodv@alum.mit.edu

Abstract. Much of modern cryptography is predicated on the assumption that users have secrets which are generated using perfect randomness, and kept perfectly secret from an attacker. The attacker is then constrained to black-box (input/output) access to the user's program. In reality, neither assumption holds, as evidenced by numerous side-channel attacks that have surfaced over the last few decades.

This leads naturally to the question – is it possible to secure cryptography against general types of information leakage at a fundamental, algorithmic level (as opposed to, say, solutions for specific attacks)? This is the goal of leakage-resilient cryptography.

In this talk, we will survey recent developments in leakage-resilient cryptography, including definitions and constructions of various cryptographic primitives secure against general forms of leakage. We will place particular emphasis on the new tools and techniques that we have developed to handle information leakage, as well as the relation between leakage-resilience and other questions in cryptography.

D. Catalano et al. (Eds.): PKC 2011, LNCS 6571, p. 283, 2011.