Adi Shamir
4 mai 2011

How Cryptosystems are Really Broken

Abstract:

Most of the cryptosystems we currently use are highly secure, and cannot be broken by mathematical cryptanalysis. However, over the last fifteen years researchers have developed many types of physical attacks on their implementation which can easily bypass their mathematical security.

In this talk I will survey some of these techniques, and show how difficult it is to build a truly secure communication system.