Provable Security for Public Key Schemes

Jürgen Ecker[1] <juergen.ecker@fh-hagenberg.at>

For centuries cryptosystems were considered secure if they could not be broken for a long time. Of course, the lack of a counter example at hand is not a proof for security and even today there are examples of cryptosystems that are finally broken after more than ten years. In order to guarantee security over a long period, it seems desirable to have a proof for the security of the system. Typically, a proof of security is a "reduction", a break of the system leads to a solution of a theoretical problem (like factoring a number or computing a discrete logarithm) which is considered (complexity theoretically) hard. The first and maybe most important step in proving the security of a cryptosystem is to define what a secure cryptosystem is. This includes a description of what an attacker can do (gets to know) and what precisely his goal is. The second step is to prove that a cryptosystem actually has the desired security properties.
In this talk important security definitions such as indistinguishability, semantic security, and non-malleability for public key cryptosystems under adaptive and non-adaptive chosen cipher text attacks are compared, and cryptosystems with a security proof are presented.

[1]FH Hagenberg, Computer- und Mediensicherheit