Specific versus General Assumptions in Cryptography

Russell Impagliazzo, CSE Department, UCSD *

December 19, 2013

Abstract

Modern cryptography began with the insight that computational difficulty could limit the ability of an attacker to break encryption or forge signatures. However, it was not for another few years that the required computational difficulty of specific problems on specific distributions for a cryptographic protocol to be secure was made explicit and quantitative. A further advantage of formalizing this connection is that it clarifies the exact properties, both in terms of which aspects should be computationally feasible and which related problems should be computationally intractable, were used to prove security of the protocol. This lays the foundation for proving possibility results in cryptography based on general assumptions, about the existence of types of cryptographically useful tools, rather than based on the difficulty of specific problems. A pattern emerged, where a new cryptographic goal is proposed, an " existence proof" given based on specific assumptions (sometimes untested) is given, then a variety of protocols are given based on different assumptions, and then these protocols are abstracted in terms of more general assumptions that suffice.

This talk will focus on the history of how this pattern emerged, the advantages that proofs of security based on general assumptions gives over protocol design based on specific assumptions, and on both progress and set-backs in basing cryptography on general assumptions.

*Work supported by the Simons Foundation and NSF grant CCF-121351.