Brief History of the Foundations of Cryptography*

*Avi Wigderson***, Notices **55**(2008), 6-7

A brief but accurate account of the history and impact of this field

Like all areas in theoretical computer science, foundations of crypto is a mathematical discipline that studies computational notions. Its main goal is to put on firm, rigorous foundations such fundamental notions as "secret", "privacy", "knowledge", and more. Being "complexity-based", it relates the security of various protocols (for achieving diverse tasks, from secure communication, to digital signatures, electronic cash, voting, etc.) to the difficulty of solving computational problems. A typical research paper in this area proves mathematical theorems of the following nature: "The security of a protocol (both terms precisely defined) can be violated *only if* there is an efficient algorithm to a seemingly hard computational problem". The huge value of such theorems is that understanding a highly complex, counterintuitive scenario with several, adversarial parties, reduces to a clean question about the difficulty of a single function.

In the 1980s, the first decade of the field, huge progress was made on mathematically defining the subtle notions of cryptography. Moreover, it revealed the power of the assumptions underlying public-key encryption in the breakthrough papers of Diffie-Hellman and Rivest-Shamir-Adleman, which were shown to have a host of other diverse cryptographic consequences. This mathematical study was performed almost solely by theoretical computer scientists, driven mostly by good old-fashioned mathematical curiosity, the depth and subtlety of the millenia-old concepts involved, and the magical consequences of a world in which difficult problems enable, rather than disable, progress.

This body of work laid the foundation for immense practical applications of e-commerce once the Internet revolution arrived in the 1990s. And its depth and beauty attracted top mathematicians, both to find new math problems on which to base cryptosystems, as well as attack such systems by finding better algorithms for such problems. Finally, this body of work spun and enriched new fields in theoretical computer science, including pseudorandomness, interactive proofs, and computational learning theory.

In the past twenty years, this field has interacted with its applied side in the best way any area of applied math can. It incorporated new technological advances and restrictions into its models, further improved efficiency of protocols, and reduced computational assumptions. Needless to say, much more can and will be done. But perhaps foundations of cryptography has been even closer to practice than other other fields; put simply, the adversarial, unexpected nature of cryptographic scenarios almost precludes testing and intuitive grasp of protocols, thus creating a much stronger reliance on clear models and theorems.

Nevertheless, the tension between the applied and theoretical which exists in all these areas indeed exists in crypto as well, due to the natural differences in motivation of commercial applications and mathematical research. In all of them, one can bemoan the deficiencies of a mathematical model or theorem for practical application. Or instead, one can delight in the clarity, insight, guidance, and indeed, the "proofs" they provide, for practical innovation and design. Take your pick! And best of all, one should continue research, implementation and interaction.

* An extraction

** Avi Wigderson is a professor of Institute for Advanced Study (avi@ias.edu).