Letters to the Editor

Other Affordable Textbooks

This letter refers to the article in the AMS *Notices*, August 2007: "Affordable textbooks campaign: Can online texts help?" by Bernard Russo. Unfortunately, the article does not mention the texts in *Schaum's Outlines* which still sell for less than US$20.00. Let me quote from the book by Gian-Carlo Rota, *Indiscrete Thoughts*, 1997, Birkhauser Boston.

"…, every scientific bookstore from Santiago to Islamabad, from Nigeria to Indonesia to Ecuador to Greece, makes a point of shelving the nicely bound …*Schaum's Outlines*. …Why is it that these much-maligned (but far from neglected) presentations of the fundamentals of mathematics …are profitably sold in every scientific bookstore? …Why is it that Serge Lang's *Linear Algebra* …displays the sale of a few thousand copies over … fifteen years, while the same title by Seymour Lipschutz in *Schaum's Outlines* …sells a few hundred thousand copies in twenty-six languages?

"Mathematicians …would have everyone believe that the texts published under the banner of *Schaum's Outlines* are inferior products, suitable for inferior countries, inferior races, …This writer proudly acknowledges his kinship and wholehearted solidarity with those 'inferior' people who peruse the volumes of *Schaum's Outlines*. ……Anyone who is about to teach the undergraduate mathematics curriculum should come down to earth by looking through *Schuam's Outlines* before burdening the class with those well-printed, many-colored, highly-advertised hardcover volumes that are pathetically passed off as textbooks."

As the author of a linear algebra text in the *Schaum's* series, I strongly agree with the late Gian-Carlo Rota. I am very happy there is a linear algebra text online. (If a student has to pay about 5 to 10 cents to print each page, then perhaps my book at $18.95, with 475 pages, might even be cheaper.)

My other argument with textbook publishers, besides their high prices, is that they put out new editions every few years in order to stop the resale market of their texts. Mathematics does not change very much. Mathematics departments should insist with a publisher that they will adopt the publisher's textbook only if the publisher promises not to publish a new edition for at least five years. Summarizing, as supported by Gian-Carlo Rota, *Schaum's Outlines* may be fine alternatives to many of the expensive texts. I also suggest that professors should at least compare *Schaum's Outlines* with the texts that they are considering to use.

—*Seymour Lipschutz*
Temple University
seymour@temple.edu

(Received September 14, 2007)

Brief History of the Foundations of Cryptography

I have read the article "The uneasy relationship between mathematics and cryptography" by Neal Koblitz. A major part of the paper is a petulant attack against the field of research he calls "provable security", which I will call here by its standard name, foundations of cryptography. The paper contains baseless charges which are defended by imaginary, anecdotal, or self-contradictory arguments.

In this short space I cannot argue the value of rigorous proofs and asymptotic analysis for understanding practical systems. I will only attempt to fix one flaw in Koblitz' paper, and give 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, instead of slander.

—Avi Wigderson
Institute for Advanced Study
avi@ias.edu

(Received September 27, 2007)

Reply to Wigderson

Wigderson makes some serious accusations against me, but fails to indicate what in my article was "slander" or a "flaw". Was it my mentioning that cryptography papers are often rush jobs submitted a few hours before a deadline? Was it my reference to leading researchers whose claims for their protocols were based on what turned out to be fallacious proofs? Was it my discussion of the need for caution in interpreting asymptotic results in a practical setting? Was it my criticism of the use of the term "provably secure" to advertise cryptographic systems to the outside world? Wigderson should have explained to us which of these, in his opinion, was "slander" or had a "flaw".

Wigderson's brief account of the history and impact of theoretical cryptography is reasonably accurate if one makes allowances for the tradition of exaggeration and hyperbole in this field. However, the scientists and engineers who pioneered the Internet revolution would undoubtedly be surprised to hear Wigderson claim that he and his colleagues deserve credit for laying its foundations. I think they would say that the role of theoretical computer science in establishing e-commerce was very modest.

—Neal Koblitz
University of Washington
koblitz@math.washington.edu

(Received October 18, 2007)