Letters to the Editor

Koblitz Article Misleading

I found Koblitz's essay "The uneasy relationship between mathematics and cryptography" (*Notices*, Vol. 54, No. 8) misleading in several ways.

Most importantly, I believe that Koblitz's views regarding the subject are based on several fundamental misconceptions. For example, he seems to view the unfortunate (and rare) cases in which flaws were found in published claimed "proofs" (of security) as indication that proofs are useless (w.r.t. security). In my opinion, these incidences merely reinforce the importance of careful verification of proofs, which constitute our only way of distinguishing facts from conjectures. Furthermore, Koblitz often confuses proofs with what is being proved, and consequently does not distinguish between the inadequacy of the claim (e.g., an unsatisfactory definition of security) and the incorrectness of its proof. Finally, he often uses unsound reasoning (e.g., inferring that last-minute conference submissions indicate a rush to publish minor results).

The foregoing flaws dominate the series of papers by Koblitz and Menezes (see references in Koblitz's essay). For a discussion of the main flaws, the interested reader is referred to my essay `http://eprint.iacr.org/2006/461`. Let me just stress that, in contrary to Koblitz's belief, the fact that this essay does not criticize the papers of Koblitz and Menezes for inadequate references to prior work does not mean that such cases are not numerous. On the contrary. Koblitz's essay suffers from the same problems, and in addition it provides a distorted account of my own essay (e.g., the (legitimate) controversy regarding the "Random Oracle Model" is far from being the focus of my essay and was certainly not the source of my concerns regarding the Koblitz and Menezes papers).

I also wish to correct Koblitz's account of the events related to the publication of his paper with Menezes in the *Journal of Cryptography*. I did not object to the publication of the paper due to my strong disagreement with its contents, but rather due to the nature of this paper which, in my opinion, is not a novel technical contribution of the type sought by the journal. My opinion was that the paper may only be published as a "position paper". Since the authors refused to revise the title of their paper accordingly, the editor-in-chief was forced to write a special preface that explains that their paper is a position paper.

—*Oded Goldreich*
Weizmann Institute of Science
oded.goldreich@weizmann.ac.il

(Received August 27, 2007)

Koblitz Misrepresents Cryptography

In the famous joke, a mathematician would not infer the color of a sheep's right side from its left side. But Neal Koblitz, in his article on "The uneasy relationship between mathematics and cryptography" makes quite a few broad generalizations from a handful of anecdotes.

Koblitz's disparagement of security proofs is particularly misleading. Proofs of security of cryptographic protocols are standard mathematical proofs and in that sense are no more "over-hyped" (to use Koblitz's term) than proofs in calculus. Koblitz gives examples of mistakes in security proofs, but as we know such examples can be found in any area of mathematics. He also criticizes these proofs for relying on unproven conjectures. This is indeed most often the case, as is not surprising in such a young and vibrant field. Eventually we might prove these conjectures (although some seem as hard as the hardest open problems in mathematics) but regardless, it's much better to use a protocol proven secure under a well-defined and widely believed conjecture than a protocol with no analysis at all.

Koblitz points out the obvious truth that in cryptography, as in any mathematical field that models reality, the precise statement of a theorem is crucial to its practical meaning. Indeed, while we all know that the impossibility of angle trisection depends on the precise definition of allowed operations, none of us relies on this theorem to protect our credit card information. Here indeed cryptographers have sometimes misstepped and inadequately modeled the scenarios in which systems could be attacked, leading to systems that regardless of their formal analysis were insecure in practice. But the problem is not inherently with proofs of security but rather with cryptography itself, a notoriously difficult subject which over its long history has seen many great minds miss subtle points and design systems that were eventually broken.

In fact, the only way to systematically improve practical security is to insist on precise modeling, and study these models using mathematical proofs, on the way refining the models and identifying and correcting subtle weaknesses in protocols. Indeed, Koblitz's anecdote on the MQV and HMQV protocols demonstrates precisely how careful definitions and insistence on proofs can direct an incremental process towards more secure protocols.

—*Boaz Barak*
Princeton University
boaz@cs.princeton.edu

(Received August 30, 2007)

Publication of Koblitz's Article Questioned

I was shocked and dismayed that the *AMS Notices* published Neal Koblitz's article ["The uneasy relationship between mathematics and cryptography", September 2007] without, apparently, any editorial oversight. As one who works in the field of "provable security", I vehemently disagree with Koblitz's main argument—more on this below—but this is not my primary complaint. Instead, what I found abhorrent is that the article crosses the line from academic argument to personal screed, from constructive criticism to belligerent name-calling. I cannot imagine the *Notices* publishing a similarly disparaging article about any other academic discipline.

By another fault of the editors, readers were not given the opportunity to read a companion article containing a countervailing point of view. Without dissecting Koblitz's arguments point-by-point, let me assure readers that proofs in modern cryptography are as meaningful as proofs in any other field. Can a scheme that has been proven secure still succumb to a real-world attack? Yes, but this does not invalidate the proof. (A proof is given with respect to a particular definition; any single definition is not appropriate for all possible environments in which a scheme may be deployed.) Are most results in cryptography conditional? Yes, but this has been shown to be inherent until the P vs. NP question is settled, and should not hold back research. Do mistakes happen? Occasionally, though rarely. But this surely does not diminish the importance of proofs in the first place.

Frankly, I cannot understand why any mathematician would discourage the use of definitions, proofs, and formal reasoning in any field. (Indeed, these elements have helped cryptography progress from an art to a science.) Koblitz's article clarifies his motivation: sheer elitism. According to Koblitz, cryptographers publish papers of "little originality" and containing "tiny improvements"; when we do publish something of potential interest, it is likely to be wrong. According to Koblitz, cryptographers are simply incapable of writing correct proofs, hence his admonition that anyone other than "trained mathematicians" simply give up on the goal. This is snobbery at its purest.

Publication of Koblitz's article has the potential to cause serious damage: not to the field of cryptography—which will continue to do fine with or without Koblitz's support—but to the future involvement of mathematicians in this field. In the future, the editors should more carefully weight the pros and cons of publishing "contributions" of this nature.

—*Jonathan Katz*
University of Maryland
jkatz@cs.umd.edu

(Received August 30, 2007

Koblitz's Arguments Disingenuous

Addressing Neal Koblitz's disingenuous arguments against theoretical cryptography in his recent article in the *Notices* requires far more elaboration than allowed by the space allocated for this letter (see http://www.ee.technion.ac.il/~hugo/ams-letter). Let me thus focus only on some of Koblitz's unfounded claims against my work on the HMQV protocol that he uses as a way to discredit the entire field of complexity-based cryptography (what he refers to as "provable security") and to deny the significant achievements of this field, in particular its important contributions to the practice of cryptography.

Contrary to what Koblitz claims, the HMQV work represents a prime example of the success of theoretical cryptography, not only in laying rigorous mathematical foundations for cryptography at large, but also in its ability to guide us in the design of truly practical solutions to real-world problems. Indeed, the HMQV key-agreement protocol that resulted from this work not only improved significantly on its predecessor, the MQV protocol, in terms of analysis and security guarantees, but the protocol itself became more practical, improving performance and lowering the dependency on external mechanisms such as trust in certification authorities and key derivation functions.

This double improvement, in both security and performance, is no coincidence. It is the very understanding that one obtains through the process of formally proving (or disproving) a cryptographic protocol that allows us to eliminate safety margins that are often added to cryptographic schemes when there is not enough confidence in the strength of the design. The success of this "proof-driven design" methodology is a testament to the fundamental role of the theory of cryptography in bringing more secure systems to practice.

There is no better way to assess the value of the HMQV protocol than reading the paper itself posted under http://eprint.iacr.org/2005/176. In particular, the introduction and concluding remarks section in the paper, unchanged since the original publication, already contain answers to many of the points raised by Koblitz against our methodology. Also note the preface where I comment on a correction pointed out by Alfred Menezes that, contrary to Koblitz's misleading account, did not change in any essential way the results and value of the work, neither with respect to its provability nor the substantial practical benefits of HMQV.

Let me end by stressing a very important point in understanding the role of theory when designing and analyzing real-world cryptographic systems: By its very nature, there is no (and cannot be) empirical evidence for the security of a design. Indeed, no concrete measurements or simulations can show that attacks against a cryptographic scheme are not feasible. The only way to do so is to develop a formal mathematical model and language in which to reason about such schemes. The area of theoretical cryptography and its applications has been remarkably successful in developing such models. They are certainly not perfect and will be further improved over time, but the foundations laid so far are outstanding. Whoever finds them insufficient should be encouraged to improve upon them or come up with alternatives. Emotional and unfounded attacks against a whole research area and its individuals, as carried by Koblitz, are of no use.

—*Hugo Krawczyk*
IBM T. J. Watson Research Center
hugo@ee.technion.ac.il

(Received September 3, 2007)

Reply to Katz, Goldreich, and Krawczyk

Jonathan Katz misstates what I wrote in my article and attributes to me things I never said, all to justify accusing me of "sheer elitism" and "snobbery at its purest". I never objected to cryptographers making a carefully reasoned, rigorous argument in support of a claim. Indeed, in my papers with Menezes on "provable security" we give detailed explanations of the need for precision in definitions and security analysis, and we describe some of the best examples of early and more recent research along these lines. In my article what I took issue with was all the hype, misleading terminology, and easily misunderstood and misinterpreted "theorems" that one finds in much of the "provable security" literature. It is hard to escape the impression that mathematical jargon and the theorem-proof paradigm are often used to kick dust in the eyes of outsiders.

It is Oded Goldreich, not me, who gives a misleading version of the events surrounding his last-minute effort to prevent publication of my article with Menezes in the *Journal of Cryptology*. Our paper had gone through the refereeing process almost two years before, and had been judged to be of sufficient technical novelty to merit acceptance. Goldreich's essay "On post-modern cryptography" finds fault with our article not on technical, but rather on philosophical grounds. Calling Menezes and me "post-modern [and] reactionary", he is incensed by some of our conclusions—notably, that "our confidence in the random oracle assumption is unshaken" and that cryptography "is as much an art as a science". Whatever Goldreich's reasons might have been for attempting to block our article on the eve of its publication, in the scientific world such conduct by an editorial board member is irregular and improper.

Hugo Krawczyk's letter itself is an illustration of what I find so exasperating in the "provable security" field. In order to advertise his work as "a prime example of the success of theoretical cryptography," Krawczyk minimizes the fact that his published proof was fallacious. If the HMQV protocol had been deployed in its original form as published, not only would the advertised "provable security" guarantee have been false, but in certain settings HMQV could have been breached by a malicious adversary. That's not a minor matter. (See `http://eprint.iacr.org/2005/205` for detailed explanations of the security flaws that have been found in HMQV.) Indeed, if Krawczyk believes that fallacies in proofs are so unimportant, then why bother to give proofs at all?

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

(Received September 14, 2007)