September 2, 2007

Notices of the AMS, Editor
Email: notices@math.ou.edu

Dear Editor,

Having read Neal Koblitz's article in the recent issue of the Notices of the AMS, I find it necessary to respond to some of the untrue and misleading comments made by Koblitz in that article. This includes a blatant attempt to discredit the entire field of complexity-based cryptography and to deny the significant achievements of this field, in particular its important contributions to the practice of cryptography. The article also includes a personal attack on my work and conduct, specifically in reference to the development and analysis of the HMQV protocol, that I cannot ignore.

As a matter of fact, the *true* story of the HMQV protocol serves as a great example of the usefulness and relevance of theoretical cryptography to the real world, in full opposition to Koblitz's thesis, and therefore I will focus my comments on the HMQV work.

The basis for that work was an analysis I performed in 2004, using formal tools developed in previous years, on the Menezes-Qu-Vanstone (MQV) protocol, one of the most efficient key exchange schemes in the literature and widely documented in cryptographic standards. The results of my analysis were twofold. First, the MQV protocol, while based on some remarkable ideas, could not be proven secure in the formal models I was using. Moreover, these analytical weaknesses translated into actual shortcomings of the protocol's security (some of which were known before my work). Second, and this is the main contribution of my work, I modified MQV into a new protocol, named HMQV, that preserved the exceptional performance of the original protocol but now with a well-defined set of security properties all backed by formal analysis.

Very significantly, and this is a theme central to our field, not only the analysis and security guarantees were improved but actually the protocol itself became more practical, improving on 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 (or what Koblitz refers to as "provable security") in bringing more secure systems to practice.

In his attempt to invalidate my results (and with them the whole approach of "provable security"), Koblitz claims that if the results in my paper – and the consequent advantages of HMQV over MQV – were valid, it would have been a cause for major embarrassment for the MQV authors and even for the NSA that licensed the protocol. Well, the results were and are valid (with a correction pointed out by Menezes that did not change the results and value of the work in any substantial way) and yet there is no room for embarrassment. To the contrary, the MQV protocol is a remarkable and influential piece of work. It is only natural and expected that 10 years later (MQV was designed in 1995) our understanding of protocol design and analysis had improved, especially in a young and vibrant field as ours. The HMQV protocol uses all the ideas and intuitions that were the basis of MQV, but interprets and optimizes them using 2005 state-of-the-art knowledge. This is exactly the type of fundamental new insights gained by "provable security" that Koblitz so vehemently dismisses.

In the short space that I have for this letter it is impossible to enter technical details in order to make the above issues more clear and concrete. The interested reader is invited to consult my paper that has been posted since its publication in `http://eprint.iacr.org/2005/176.` I did not modify the paper since its original posting, but I have added a preface referring to a gap in one of the proofs that was pointed out by Alfred Menezes. This resulted in a correction, only needed in certain variants of the protocol, but it 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.[1]

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 very successful in developing such models. They are certainly not perfect and will be further improved over time, but the foundations laid so far are remarkable. 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.

Yours Sincerely,

Hugo Krawczyk
IBM T.J. Watson Research Center

[1] Menezes' correction required *no* change to the core protocol, while a single prime-order test was needed in some extensions; even in these cases the performance of HMQV is same or better than MQV's. In *all* cases HMQV dispenses of two major MQV requirements from the certification authority (which may be hard, and sometimes impossible, to enforce in commercial applications): public key validation (which Koblitz considers indispensable) and "proof of possession" of the private key. The details are in the paper.