August 10, 2014

Response to Crypto 2014 Paper by Gaži, Pietrzak, and Rybár

by Neal Koblitz and Alfred Menezes

The purpose of this note is to correct some erroneous or misleading statements in the Abstract and Introduction to the Crypto 2014 paper "The Exact PRF-security of NMAC and HMAC" by Gaži, Pietrzak, and Rybár (GPR).

1. The first paragraph of the subsection "Our Contributions" states:

> Our first contribution is a simpler, uniform, and as we will show, basically tight proof for the PRF-security of NMAC^f assuming only that f is a PRF: If f is an ϵ-secure PRF against q queries, then NMAC^f is roughly $\ell q\epsilon$-secure against q queries of length at most ℓ blocks each.

However, GPR fails to note that a very similar result giving $\ell q\epsilon$-security was proved earlier in our paper "Another look at HMAC." GPR acknowledges our main theorem, which gives $\ell\epsilon$-security under a stronger PRF-assumption, but omits any mention of our Corollary 10.3, where we proved that $\ell q\epsilon$-security under the weaker assumption follows from the theorem. GPR can correctly claim that their result is a new contribution, because it is "more fine-grained" (in the authors' words) than the general $\ell q\epsilon$-security property that we proved in Corollary 10.3. However, failure to adequately acknowledge prior work is a serious lapse.[1]

2. GPR rightly criticize us for an error in a preliminary version of our HMAC paper. But they fail to note that there's a published version of the paper that does not make any incorrect claim. Our HMAC paper appeared in the October 2013 issue of *J. Math. Cryptology* (published online 25/9/2013) several months before the submission deadline for Crypto 2014. However, GPR do not reference the published version in their bibliography. It is quite peculiar to criticize a preliminary version of a paper and omit any reference to the final published version.

3. These two lapses may be the result of carelessness rather than any deliberate attempt to mislead. There is evidence that the GPR paper was written in haste and was not adequately checked by either the authors or the Crypto 2014 referees. For example:

a. The abstract states that "NMAC was introduced by Bellare, Canetti and Krawczyk [Crypto '96], who proved it to be a secure pseudorandom function (PRF)," and this statement is repeated in the third paragraph of the Introduction. This is wrong, as is well

[1] On the other hand, we do not mean to imply that the question of who first gave a uniform proof of $\ell q\epsilon$-security of NMAC is of any importance. As we said in Remark 10.5 of our HMAC paper, "As far as we know, our proof of Corollary 10.3 is the first uniform proof of $O(nq\epsilon)$-security [$O(\ell q\epsilon)$-security in the GPR notation] of NMAC assuming ϵ-security of f in the usual sense. Of course, in view of the huge tightness gap of order nq one can justifiably respond to our claim by saying 'Who cares?'"

known. The Crypto 1996 paper proved only that NMAC has the secure-MAC property, which is much weaker than the secure-PRF property.

b. The abstract states that the GPR bound "is basically tight." This is wrong. In reductionist security proofs, tightness means that the success probability and running time are basically preserved in the reduction. An $\ell q\epsilon$-security result has a gigantic tightness gap of ℓq. In our HMAC paper we comment that a result with such a large tightness gap is of little use in practice because it gives a meaningless security guarantee. In their Introduction, GPR repeat the erroneous claim that their bound is "basically tight." What they undoubtedly meant to say is that their bound is *optimal* in the sense that it cannot be improved (unless one strengthens the assumption). But "optimal" and "tight" mean very different things.

4. GPR disparage our theorem giving $\ell\epsilon$-security of NMAC because it is based on what they call a "non-standard" PRF assumption (what we call the "strong PRF property"). In our paper we discuss the rationale for using the strong PRF property, namely, one needs it in order to get a bound with a substantially lower tightness gap. Of course, if one has no interest in the practical meaning of the bounds, then one can ignore our $\ell\epsilon$-result and be satisfied with an $\ell q\epsilon$-bound under the weaker PRF-assumption.

5. GPR try to minimize the significance of the defect we found in Bellare's Crypto 2006 paper, insisting that the only thing wrong with it was that he was "overoptimistic" in interpreting his results. In reality, his interpretation is simply wrong, because it would make sense only if his proof were uniform. As we show in §8 of our HMAC paper, a correct interpretation of Bellare's main theorem, taking into account the non-uniform "coin-fixing" step, gives a result that is useless in practice.

The unfortunate consequence of Bellare's use of coin-fixing in his proof is that it forces him to assume an extremely strong PRF property. Namely, the compression function $f(K, M)$ must be ϵ-secure even against an extraordinarily powerful adversary that gets advice strings that depend on f — for example, the adversary can be hardwired with messages M_0 such that $f(K, M_0)$ has unusual behavior as K varies.

Moreover, nowhere in Bellare's Crypto 2006 paper is the reader alerted to the fact that the proof of the main theorem is non-uniform and the hypothesis of the theorem assumes security against non-uniform adversaries. On the contrary, as we explain in §7 of our HMAC paper, certain comments in the early sections of Bellare's paper — especially in the discussion of how to interpret his bounds — would make sense only if the proof in his paper were uniform. Obviously this confusion results not from a deliberate desire to mislead the reader, but rather from an honest mistake on the part of the author, albeit a serious one.

6. GPR again try to minimize the significance of the flawed reasoning in Bellare's Crypto 2006 paper by claiming that such "overoptimism" was common in provable security papers at the time. According to GPR, the consequence of allowing non-uniform adversaries "was not widely known in the crypto community and overoptimistic estimates for the exact

security implied by non-uniform reductions have appeared in numerous papers." They do not cite any such papers, and most likely their statement is wrong. As we comment in the Introduction to our paper "Another look at non-uniformity," security reductions that use coin-fixing are very rare; almost all reductionist security proofs are valid in the uniform model. In an extensive search of the literature we could find only three other examples besides Bellare's paper where authors made erroneous interpretations of results obtained with a non-uniform proof. In one case (three papers by the same author, see [35,36,37] in the bibliography of our HMAC paper) the author directly carried over the method of proof in Bellare's paper to his setting, without realizing the implications of the coin-fixing. In another case (reference [16] in our HMAC paper) the authors used Bellare's result without realizing that this caused their own result to lose validity in the uniform model. The only example we could find that was independent of Bellare's proof was a paper by Dziembowski and Pietrzak that used coin-fixing in the context of leakage-resilience (reference [14] in our HMAC paper). It is a gross exaggeration for Gaži, Pietrzak, and Rybár to suggest that mistaken interpretations of non-uniform results were common in the crypto community. To the best of our knowledge there is only one example of this that is independent of Bellare's paper, namely, the Dziembowski–Pietrzak paper.

7. GPR state that awareness of the dangers of "overoptimistic estimates for the exact security implied by non-uniform reductions" date "at the latest" to 2010, when a Crypto paper by De, Trevisan, and Tulsiani "discuss this issue in detail." This is incorrect. The De–Trevisan–Tulsiani paper says nothing about faulty interpretations of non-uniform security reductions. As far as we know, the first place where a critique of flawed analysis of non-uniform provable security appeared was our HMAC paper (first posted 19/2/2012).

Finally, we note that all of the errors and misleading statements discussed above appeared in the Abstract and Introduction to the GPR paper. Although one cannot expect Crypto referees to meticulously examine technical proofs, one would hope that they would carefully read at least the abstracts and introductions to submitted papers. When embarrassing mistakes appear in prominent places in the final Crypto proceedings, that does nothing to enhance the prestige of the conference.