From: (b) (6)
To: Petzoldt, Albrecht R. (IntlAssoc); Perlner, Ray A. (Fed)
Subject: SRP attack
Date: Tuesday, October 31, 2017 2:04:42 PM

Hi, guys,

I will finally start to edit the HFEv- stuff this week and next. I apologize for being so negligent. Unfortunately I'm immature and if something is not in front of my eyes, I think that it doesn't exist.

I have another item of business I want to address, though. It occurred to me that we may have an error in our SRP attack paper. I'm not sure if it is too late to address this before the article is in press, but in the past it has taken several months before the SAC proceedings are published. I'm hoping that there is still time to address the error.

The error is in the theorem deriving the Hilbert Series for the minrank system. The Hilbert Series can't be a polynomial because that would mean that the ideal is zero-dimensional and that only the trivial solution exists, whereas one of our assumptions is that the ideal is positive dimensional. It is a stupid error that I already made with Ray once. The argument is not so bad except that we know that the span of the minors must have corank at least one. So given our heuristic that the minors occupy the largest possible subspace, the Hilbert Series should be $HS(t)=(1+(m-1)t-(m-1)t^2)/(1-t)$.
This still produces a Hilbert regularity of 2, and thus the degree of regularity is 2 as we claimed.

Albrecht, do you know how to contact the editors to indicate that we found an error that neither the referees nor we caught? It is simple to fix (only a few lines) and doesn't affect the result much, but the details are wrong.

Cheers,
Daniel