From:	Emanuel Knill
To:	Miller, Carl A. (Fed)
Subject:	Re: BERB review
Date:	Friday, April 21, 2017 2:51:26 PM

On Friday 21 April 2017 11:30:14 you wrote:
> Here's my review for your QCRYPT abstract. Interesting reading! It's
> nice to know more about the adaptive style of randomness generation that
> you talked about.

Thanks for the review!

> I'm interested in the way you bound randomness (here and also in the last
> paper I reviewed for you) – it avoids the need for Azuma-inequality
> arguments (I think?) and it seems to more closely resemble the methods
> that are used to prove security against quantum side information.

Given the final form of the bounds for entropy accumulation and how it is applied, it seems to me that the entropy-accumulation arguments with max-tradeoff functions parallel and recover large deviation bounds (in an interesting way) and in this sense the corresponding bounds seem more closely related to Azuma-Hoeffding than to test-supermartingales, which is what we use. Of course, test-supermartingales are at the foundation of many large-deviation arguments, so the relationships are always closer than it might appear.

Direct bounds based on test supermartingales are generically better than what you can get by Azuma-Hoeffding inequalities (on average). This is explicitly visible in the case of testing LR. Azuma-Hoeffding is optimal only for binary statistics. One could take advantage of Bernstein-like bounds to exploit small empirical variances, though it makes the usual bounds even more involved, and I haven't seen anyone do this. I suppose if I didn't have test supermartingales, I would develop Bernstein-like methods. The main slack in our techniques is that allowing for not knowing the number of trials (or rounds) ahead of time comes at a small cost (related to the law of the iterated logarithm) compared to what might optimally be achievable. Is is typically not easy to get that extra gain, with binary statistics being an exception. For our applications, the best statistics are rarely binary.

> It
> might be interesting to explore the connection to the quantum side
> information arguments. I'm busy with some submissions right now (also
> submitting to QCRYPT) but it would be fun to talk more about this some
> time.

I'll tell you what I know when I visit.

Manny

>
> -Carl
>

> ——————
> Carl A. Miller
> Mathematician, Computer Security Division
> National Institute of Standards and Technology
> Gaithersburg, MD
>
>
>
> On 4/21/17, 1:09 PM, "Canon_C7065@nist.gov" <Canon_C7065@nist.gov> wrote:
>
>
>