From: Miller, Carl A. (Fed)
To: Knill, Emanuel H. (Fed)
Cc: Peralta, Rene C. (Fed)
Subject: Re: WERB review
Date: Thursday, March 9, 2017 4:32:20 PM

Hi Manny—

Thanks a lot for taking care of this. Your stylistic suggestions sound good, I'll keep them in mind when revising.

Re. the comparison between sequential and parallel: I believe that the parallel setting is strictly more general. If a device takes inputs x_1, \ldots, x_n in sequence and generates outputs a_1, \ldots, a_n, that entire process can be simulated by a device that accepts (x_1, \ldots, x_n) all at once and generates output (a_1, \ldots, a_n) all at once. (There may be some subtleties in describing exactly what this process looks like, but I don't think that's crucial.) Stated differently, we can enforce commutativity in the sequential case if we want: just copy the outcomes a_1, …, a_n sequentially into registers A_1, …, A_n and then measure the registers A_1, \ldots, A_n all at once. That amounts to a collection of commuting measurements. (But it's possible that I'm overlooking something.)

Looking forward to presenting this next week. See you later!

-Carl

_____
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

On 3/9/17, 3:25 PM, "Emanuel Knill" <emanuel.knill@nist.gov> wrote:

> Hi Carl,
>
> I went ahead and approved the paper.
>
> A few comments:
>
> I would spell out QKD in the title.
>
> It would be nice if the overview made it clear what role ϵ
> plays and how it relates to the relevant error/smoothness parameter.
> I didn't notice this in the overview, perhaps I missed it. In any
> case, I had to look up the theorem to realize that ϵ can be
> made constant and error decreases exponentially to zero with N. Did
> I interpret this correctly? Normally when I see ϵ's I expect
> that there are reasons to make them arbitrarily small. In this case,
> is there a reason?
>
> Do we need fairly good quantum states or is this robust down
> to a limit with separable states?
>
> I guess my interpretation of what you do is to show that diqkd is
> possible with one round of state -> measurement. For me this is
> neither a weakening nor a strengthening of the multi-round

situation. In the sense that the overall state -> measurement obtained from multiple rounds is neither a special case nor a generalization of the same thing for one round. For example, the multi-round case as I define it does not make a global commutativity restriction between measurements at multiple rounds, so measurements are in a sense less constrained. But this perspective seems to depend on not restricting the game/scoring function to a specific one. Is it possible that the issues change substantially when one considers the state/measurement etc. constraints with respect to all certification schemes and (for completeness) achievable configurations rather than with respect to a specific scoring function?

I am pretty sure you didn't mean to restrict states to "automorphisms" of quantum registers, defined as being Hilbert spaces. Your definitions are to me unconventional, even if you say "endomorphisms", for several reasons, not the least of which is that states are by definition dual to observables, so are not primarily linear maps on a Hilbert space, even if they are often called "density operators". But also, why not say explicitly "positive semidefinite Hermitian operators"? Sure, Hermitian (or self-adjoint) is usually implicit in the definition of "positive semidefinite", but it doesn't hurt to make it explicit. Part of the issue I see is that confusing states with operators leads to conceptual problems, even if mathematically, in context, such a correspondence exists (modulo complications in infinite dimension).

See you,

Manny

On Monday, March 06, 2017 08:35:37 AM Miller, Carl A. wrote:
> Hi Manny & Rene –
>
> Thanks a lot for agreeing to do a WERB review of my paper (“Parallel
> Device-Independent QKD”). I just initiated the WERB process online at
> nike.nist.gov.
> If it’s possible to take care of the review by this Saturday (March 11th)
> that would be great. (I’m giving a talk about the paper next week.) I
> realize the timing is tight and I very much appreciate your help.
> Talk to you later!
>
> -Carl
>
> _____
> Carl A. Miller
> Mathematician, Computer Security Division
> National Institute of Standards and Technology
> Gaithersburg, MD
>
>