From: Miller, Carl A. (Fed)
To: Knill, Emanuel H. (Fed)
Subject: BERB review
Date: Friday, April 21, 2017 1:30:14 PM
Attachments: 3764_001.pdf

Hi Manny –

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.

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. 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.

-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: