From: Liu, Yi-Kai (Fed)
To: Knill, Emanuel H. (Fed)
Cc: Knill, Emanuel H. (Fed); Shalm, Krister (Assoc); (b) (6) [redacted]
Subject: Re: Fw: parallel randomness extractors
Date: Wednesday, February 6, 2019 2:18:12 PM

Ah. Yes, you're right... if you take the experiment and split it into L blocks, each block needs enough trials to guarantee soundness at the epsilon/L level, even though we're only trying to extract 1/L times as much entropy from each block. So for the whole experiment, the cost of guaranteeing soundness blows up by (more than) a factor of L. In practical terms, that looks pretty bad for the parameters in the NIST experiment.

Oh well...

--Yi-Kai

From: Emanuel Knill <knill@boulder.nist.gov>
Sent: Tuesday, February 5, 2019 4:01 PM
To: Liu, Yi-Kai (Fed)
Cc: Knill, Emanuel H. (Fed); Shalm, Krister (Assoc); (b) (6) [redacted]
Subject: Re: Fw: parallel randomness extractors

Wouldn't that mean that if I want an overall soundness of epsilon, I need the soundness for each block to be epsilon/#blocks? The minimum number of trials required for soundness epsilon grows as epsilon shrinks, and this would apply to each block. In addition, you have to watch for indirectly leaking information about which blocks "succeeded". You might want to look at the composability discussion in the "soundness" section of our quantum probability estimation paper.

Manny

On Tuesday 05 February 2019 13:27:40 Liu, Yi-Kai (Fed) wrote:
> I agree, the certificate doesn't show that the min-entropy is evenly
> distributed. But I was thinking you could generate a separate certificate
> for each block? You might not be able to certify every block, but you
> should be able to certify most of them?
>
> Sorry if I am going down a path you have already explored. :(
>
> --Yi-Kai
>
> ________________________________
> From: Emanuel Knill <knill@boulder.nist.gov>
> Sent: Tuesday, February 5, 2019 2:33:43 PM
> To: Shalm, Krister (Assoc); (b) (6) [redacted]
> Cc: Liu, Yi-Kai (Fed)
> Subject: Re: Fw: parallel randomness extractors
>
> We cannot certify the block property that Yi-Kai assumes. The
> certificate doesn't guarantee that the min-entropy is evenly
> distributed in this way. And I don't see how to modify our strategies
> to assure such an even distribution of min-entropy.
>
> Manny

>
> On Tuesday 05 February 2019 10:36:41 Shalm, Krister (Assoc) wrote:
> > From: Nam, Sae Woo (Fed)
> > Sent: Tuesday, February 5, 2019 9:11 AM
> > To: Shalm, Krister (Assoc)
> > Subject: Fw: parallel randomness extractors
> >
> >
> >
> >
> >
> >
> > FYI
> > ____
> > From: Liu, Yi-Kai (Fed)
> > Sent: Monday, February 4, 2019 10:31 PM
> > To: Nam, Sae Woo (Fed)
> > Subject: parallel randomness extractors
> >
> > Hi Sae Woo,
> >
> > I just wanted to follow up on your question, when we were talking last
> > week at the DOE meeting... is there a way to parallelize the Trevisan
> > extractor?
> >
> > I believe there is a simple trick that might work in your situation:
> > (I'm not sure if you've tried this already?)
> >
> > Suppose you run the Bell experiment for about 512 seconds, and get a
> > data record that has about 512 bits of min-entropy. (I'm just borrowing
> > the numbers from
> > https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.or
> >g%2Fabs%2F1812.07786&amp;data=02%7C01%7Cyi-kai.liu%40nist.gov%7Cff29083cd6
> >5f4bf6729208d68ba10430%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C636849
> >921015901164&amp;sdata=gsohVtjj1s5j%2Fig48BDDWKycSbPflYtn04LdQXKtP6E%3D&am
> >p;reserved=0 .)
> >
> > Actually, this data record has a stronger property -- you can split it
> > into L blocks, where each block has 512/L bits of min-entropy,
> > conditioned on the previous blocks. This follows from the causality
> > structure of the Bell test. This is called a "block source."
> >
> > In this situation, you can extract entropy by running the Trevisan
> > extractor in *parallel* on each block. This can be proven secure against
> > adversaries with quantum side-information, see theorem IV.2 in
> >
> > https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.or
> >g%2Fabs%2Fquant-ph%2F0608101&amp;data=02%7C01%7Cyi-kai.liu%40nist.gov%7Cff
> >29083cd65f4bf6729208d68ba10430%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%
> >7C636849921015901164&amp;sdata=13JdzR%2BMMMDP9leMKwlVCm8h4gj00iWWexILqyZKM
> >0Q%3D&amp;reserved=0 .
> >
> > Note: that paper is quite old, and the bounds are probably not optimal
> > -- in particular, they show that you can extract some (but not all) of
> > the entropy from each block. But that might be good enough to be
> > practically useful.
> >

> > Also, note that you can invoke theorem IV.2 with *any* strong extractor
> > that is secure against classical adversaries. You don't have to use the
> > Trevisan extractor. For example, you could instead use a Toeplitz hash
> > function, which has a much longer seed, but it also much faster to
> > compute.
> >
> > Finally, if you want to ask an expert on randomness extractors, you
> > could try Chris Umans at Caltech. He might be able to recommend some
> > other extractors that would be suitable for your needs.
> >
> > I hope this helps...
> >
> > Cheers,
> >
> > --Yi-Kai
>