From:	Liu, Yi-Kai (Fed)
To:	Jordan, Stephen P (Fed)
Subject:	pseudorandom generators with exponential security
Date:	Thursday, April 6, 2017 8:45:11 AM

Hi Stephen,

I looked into it some more, and I am fairly confident that if one assumes the existence of a one-way function with exponential security, then one can construct a pseudorandom generator with exponential security.

The kind of result was originally proved by Hastad et al, however this later paper by Holenstein addresses the question of exponential security more explicitly:

T. Holenstein, "Pseudorandom Generators from One-Way Functions: A Simple Construction for Any Hardness," TCC 2006.

ftp://ftp.inf.ethz.ch/pub/crypto/publications/Holens06.pdf

See the paragraph after Corollary 2. Note that he constructs a PRG that expands by one bit, but this can be iterated to get an exponentially long output.

I think this construction is quantum-secure, based on some comments by Mark Zhandry (https://www.cs.princeton.edu/~mzhandry/docs/papers/QPRFs.pdf). One would have to check this, however, since Zhandry is referring to the original security proof by Hastad et al, and not the improved proof by Holenstein.

Regarding the efficiency of the construction: in order to get 2^Omega(n) bits of security, it uses O(n^5) bits of seed. Reducing the seed length to O(n) seems to be a "nontrivial" open problem. But, I think O(n^5) bits of seed is still pretty good.

Cheers,

--Yi-Kai