From:	Peralta, Rene (Fed)
To:	circuit_complexity
Subject:	Fw: Some results on Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic
Date:	Friday, August 16, 2019 9:40:15 AM

We may want to start looking at quantum circuits.
See the 854 paper.

Rene.

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Friday, August 2, 2019 3:32 PM
To: internal-pqc <internal-pqc@nist.gov>
Cc: Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Subject: Some results on Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic

FYI. Here are a couple of papers on quantum cryptanalysis of AES, hash and PK systems, which were released recently.

https://arxiv.org/pdf/1902.02332.pdf

https://eprint.iacr.org/2019/854.pdf

Lily