From: Kelsey, John M. (Fed)
To: internal-pqc
Subject: Tests for variable timing code
Date: Friday, October 8, 2021 10:26:55 AM

Everyone,

I know there are some software tools to test crypto code to see if its timing is data-dependent (or secret-data-dependent). I've been talking to Chris Celi in the CVAP about whether it would be possible to add this to some of our automated algorithm testing for FIPS approval. Is there a good reference or linkfarm somewhere for existing tools that people have built? I'd like to point Chris to something useful, since I think this is a pretty important thing to add to our testing.

Thanks,

--John