From:	Apon, Daniel C. (Fed)
To:	Alperin-Sheriff, Jacob (Fed)
Subject:	Re: Outstanding questions about lattice OW-CPA
Date:	Tuesday, February 19, 2019 3:14:33 PM

Good ol' AFRICACRYPT:

Jiang et al. [32] also provide a security reduction against a quantum adversary in the quantum random oracle model from IND-CCA security to OW-CPA security

https://eprint.iacr.org/2018/230.pdf bottom of page 12

From: Apon, Daniel C. (Fed)
Sent: Tuesday, February 19, 2019 3:10:32 PM
To: Alperin-Sheriff, Jacob (Fed)
Subject: Re: Outstanding questions about lattice OW-CPA

I will check their spec to confirm

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, February 19, 2019 3:04:52 PM
To: Apon, Daniel C. (Fed)
Subject: Re: Outstanding questions about lattice OW-CPA

Oh yeah I assume so

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Tuesday, February 19, 2019 at 1:04 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: Outstanding questions about lattice OW-CPA

I agree that OW-CPA from small-modulus LWR + a ROM transform may be possible.

Did Saber already claim this?

..should we just write the paper? It seems useful.

--Daniel