From: Danny Niu <dannyniu@hotmail.com>
Sent: Sunday, December 09, 2018 3:18 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Rainbow

Hello Rainbow team.

This is just a trivial question: Why isn't there a Rainbow-based PKE scheme? Why is it signature-only?

I mean, the core of multivariate cryptography is a bijective trapdoor function, like RSA, so it seems to me natural to use it in both directions. Is there some particular concern regarding having a Rainbow PKE?

Thanks.