From:	Chen, Lily (Fed)
To:	Smith-Tone, Daniel C. (Fed); internal-pqc
Subject:	RE: V2V
Date:	Tuesday, March 29, 2022 5:48:58 PM

This presentation was given at our conference last summer.
https://csrc.nist.gov/CSRC/media/Presentations/suitability-of-3rd-round-signature-candidates-for/images-media/session-5-bindel-suitability-vehicle.pdf

It may not answer all the questions. But it gives some data about V2V.

Lily

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Sent: Friday, March 25, 2022 10:28 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: V2V

Hi,

I have a follow-up question to one that was posted recently on the forum and I want to see what the group thinks on this issue and see what you know about the position of the larger community. This question is on vehicle-to-vehicle and vehicle-to-infrastructure communications.

It seems to me that there are several different sorts of possible V2V communication that might require different levels of security. For example, it might be desirable to have some short distance routing information shared between vehicles that can be used to manage traffic flow. That sort of information is sensitive for a longer amount of time than information related to short term collision avoidance and likely a much shorter amount of time than some vehicle-to-infrastructure communications that may relate to more detailed information about the vehicle’s general status or even passenger information.

I’m curious if research in this area incorporates different security levels for different applications, and how that might affect things from the perspective of post-quantum. Is there any interest in short term post-quantum security (maybe signatures or PKE) at a lower security level? It would be an interesting problem if there was a need for low bandwidth short-term secure schemes generically, but I’m wondering among other things if the post-quantum aspect is relevant even if there is any desire for short-term secure crypto. Does anybody know more about this stuff or where a good place might be for me to look?

Cheers,
Daniel