From:	Miller, Carl A. (Fed)
To:	Dworkin, Morris J. (Fed)
Cc:	Cooper, David (Fed); Dang, Quynh H. (Fed); Davidson, Michael S. (Fed); Apon, Daniel C. (Fed)
Subject:	Re: meeting tomorrow 9:30
Date:	Tuesday, February 12, 2019 9:49:49 AM

Hi Morrie --

Ok, thanks for the summary. What time is the next meeting?

Aside from the sections on the security proofs, the main thing I can probably help with is the algorithm description sections (although I'd need some guidance about writing style).

-Carl

_____

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

On 2/11/19, 1:03 PM, "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov> wrote:

> Hi, Carl,
>
> We mostly continued our discussion of the value of the respective security proofs; Daniel will take a closer look at the proofs for our next meeting. The next agenda item will be to assign sections of the special pub for draft text while we wait for public comments on the misuse issue. David agreed to work some more on Section 7.1 on One-Time Signature Key Reuse, but otherwise it's pretty open as to who drafts what sections.
>
> MD
>
> > On Feb 7, 2019, at 2:14 PM, Miller, Carl A. (Fed) <carl.miller@nist.gov> wrote:
> >
> > Hi all --
> >
> > I'm sorry, I'm not going to be able to meet tomorrow -- there's going to a meeting of the QuICS funding agencies at the University of Maryland, so I'll need to be there instead. I'd appreciate if you could fill me in over e-mail!
> >
> > -Carl
> >
> > _____
> > Carl A. Miller
> > Mathematician, Computer Security Division
> > National Institute of Standards and Technology
> > Gaithersburg, MD
> >
> >
> > On 2/7/19, 12:22 PM, "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov> wrote:
> >
> > Folks,
> >

> I’ve got something to take care of early tomorrow, so I’d like to delay the start of our meeting until 9:30.
>
> FYI, the request for public comments on misuse finally went out, with the deadline on April 1.
>
> MD
>