

**From:** [Bajcsy, Zuzana \(Fed\)](#)  
**To:** [Chen, Lily \(Fed\)](#)  
**Subject:** RE: Ask for some information  
**Date:** Thursday, January 31, 2019 1:54:10 PM

---

Thank you, Lily. I printed and added it to the timesheets folder.

Zuzana

---

**From:** Chen, Lily (Fed)  
**Sent:** Thursday, January 31, 2019 11:27 AM  
**To:** Bajcsy, Zuzana (Fed) <zuzana.bajcsy@nist.gov>  
**Subject:** FW: Ask for some information

Hi, Zuzana,

This is the e-mail Daniel sent on what he has worked. Let's keep the record.

Lily

**From:** Daniel Smith (b) (6)  
**Sent:** Monday, January 28, 2019 8:54 AM  
**To:** Chen, Lily (Fed) <lily.chen@nist.gov>  
**Subject:** Re: Ask for some information

Dustin mentioned that you asked if my work was on the pqc project. I think that is open to interpretation.

I have been working on understanding the significance of rank for multivariate schemes in general, so this applies to GEMS. I figured out the relationship between generic rank  $r$  systems and those with a degree bound. I have been trying to see if there is any generic technique for getting an advantage in inverting low rank schemes. So far I have found something, but it is not significant enough even for a peer-reviewed publication, I think. I am planning on writing up a note to post on eprint and running it by Ray, Yi-Kai and Dustin.

I also have been working on understanding some of the properties of LUOV better. Ward and I seem to agree that the LUOV system produces a semiregular system when we try to solve it, but Ludovic Perret says it does not. I am not sure if this is a difference in our notions of semiregular, or of what that typically means. I am working on verifying that it satisfies the definition I know of semiregular before I confront Ludovic with this and figure out if there is anything to be concerned about.

Aside from that, I have worked on revising a paper I submitted to pqcrypto and am toying with another idea for multivariate encryption (again connected to the low rank idea).

Anyway, it is all closely connected, so you can interpret it however is convenient. As I mentioned before, lost wages are not a significant concern for me (at least at this point), and nobody can

actually stop me from working when it is my hobby.

I hope this extra info is helpful.

Cheers,  
Daniel

On Mon, Jan 28, 2019 at 3:35 PM Daniel Smith (b) (6) wrote:

I was planning to work two days in the end of December and then to start again on the seventh and work full time. I guess that makes 17x8 hours that I missed, but, of course, January 14th was a weather closure. Also, it doesn't really matter for me really, since the money is not important for me. I just hope everyone there is okay and doing well.

On Mon, Jan 28, 2019 at 3:19 PM Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)> wrote:

Hi, Daniel,

We are back to the office after the 5 weeks. I am collecting information for Intermittent Employees. Can you tell whether you were planned to work during the past 5 weeks? How many hours you planned to work? I am not sure what is the general policy yet. But I need the information.

Thanks,

Lily