

**From:** [Perlner, Ray A. \(Fed\)](#)  
**To:** [Cooper, David A. \(Fed\)](#); [Kelsey, John M. \(Fed\)](#)  
**Subject:** RE: PQCrypto submission on SPHINCS+ attack?  
**Date:** Tuesday, May 10, 2022 2:29:00 PM

---

Great. Thanks!

---

**From:** Cooper, David A. (Fed) <david.cooper@nist.gov>  
**Sent:** Tuesday, May 10, 2022 2:10 PM  
**To:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>  
**Subject:** Re: PQCrypto submission on SPHINCS+ attack?

Hi Ray,

I can help some with writing the paper, if you'd prefer not to do it on your own. I made a copy of the LNCS LaTeX template, in case you haven't already started writing something.

David

On 5/10/22 11:46 AM, Perlner, Ray A. (Fed) wrote:

Hi David and John,

Would either/both of you be willing to help optimize and coauthor a paper on the SPHINCS+ attack we've been discussing? The initial submission deadline for PQCrypto is today, but I think we just need a title and abstract and can finish the paper between now and the final May 24 submission deadline provided we send something in today, which I think would be doable.

What do you all think?

Thanks,

Ray