

**From:** [Apon, Daniel C. \(Fed\)](#)  
**To:** [Sonmez Turan, Meltem \(Fed\)](#); [internal-crypto](#)  
**Cc:** [Vassilev, Apostol T. \(Fed\)](#); [Celi, Christopher T. \(Fed\)](#); [Davidson, Michael S. \(Fed\)](#)  
**Subject:** Re: Reading club tutorials on side-channel attacks  
**Date:** Monday, August 16, 2021 3:11:00 PM

---

Hey Meltem,

There are a few external people I could ask to come give an invited talk.. Let me reach out to them!

I'll also try to start a 'persistent' email thread in a few minutes here for people to discuss these issues in (if there's a better place that people will actually see when new information is posted, that's fine too)

--Daniel

---

**From:** Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>  
**Sent:** Monday, August 16, 2021 11:27 AM  
**To:** internal-crypto <internal-crypto@nist.gov>  
**Cc:** Vassilev, Apostol T. (Fed) <apostol.vassilev@nist.gov>; Celi, Christopher T. (Fed) <christopher.celi@nist.gov>; Davidson, Michael S. (Fed) <michael.davidson@nist.gov>  
**Subject:** Reading club tutorials on side-channel attacks

Thanks Daniel again for organizing today's meeting to discuss the role of side-channel attacks and countermeasures with respect to our standards.

To have productive conversations in the long run, we might benefit from having some tutorials on side-channel attacks. If you know anyone who might be interested in giving a reading club talk on this subject, please let me know.

Thanks,  
Meltem