From: Miller, Carl A. (Fed)
To: Apon, Daniel C. (Fed)
Subject: Re: Sub-review request (PKC 2022)
Date: Thursday, October 14, 2021 3:19:25 PM

Hi Daniel –

I just sent in the review – please feel free to modify (& adjust my score if it seems appropriate). A couple comments:

- I commented use of heuristic arguments in the submission (and in the Dilithium spec). I'm a little uncertain of the conventions there – I get the sense that heuristic arguments play a more important role in classical crypto papers than they do in quantum. Maybe you could check what I said there just to make sure it isn't already obvious, or offbase.
- I'm not well-read on classical crypto, but I know Dilithium pretty well. So, under "Reviewer expertise," I said "Knowledgeable."

If there's anything to discuss, just let me know.

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Date: Friday, October 8, 2021 at 5:17 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: Sub-review request (PKC 2022)

Ok.

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>

Date: Thursday, October 7, 2021 at 11:40 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Re: Sub-review request (PKC 2022)

If you think it's not very good, then stop =)

Your opinion is what matters; I don't think there's a certain expectation

---

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Thursday, October 7, 2021 3:15 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: Sub-review request (PKC 2022)

Hi Daniel –

Quick question: Is there a convention for how much the reviewers at PKC are expected to read? (E.g., at STOC, reviewers are expected to read the first 10 pages, and then they can read more if they want to.)

I was originally planning to read the whole paper, but I have to say that the writing is not very good. Thought I'd check.

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Date: Saturday, September 25, 2021 at 1:16 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: Sub-review request (PKC 2022)

Hi Daniel –

Sure – that sounds like a good opportunity. I can write a review by October 18th.

After I've read through the submission & made comments, I could probably use some help with figuring whether it meets the acceptance threshold for this particular conference. (We can discuss that.)

-Carl

--
Carl A. Miller
Mathematician, NIST Computer Security Division
Fellow, Joint Center for Quantum Information and Computer Science (QuICS)
https://camiller.iacs.umd.edu

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Date: Saturday, September 25, 2021 at 1:06 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Subject: Sub-review request (PKC 2022)

Hi Carl,

Would be willing to sub-review this paper for me?

Sub-review deadline: Monday, October 18
(This is sufficiently ahead of the actual deadline that I can meta-review your review if you'd like. Also happy to collaborate on reading the submission if you'd like..)

Title: Revisiting the Security Estimation of SelfTargetMSIS in CRYSTALS-Dilithium

Abstract:
In this paper, we reconsider the security estimation for a NIST third round lattice-based signature scheme: CRYSTALS-Dilithium. In their documentation, the authors proved that the security of the signature scheme can be based on the hardness of the following three assumptions: MLWE, MSIS and SelfTargetMSIS. While the first two are standard lattice assumptions with hardness well studied, the authors claimed that the third assumption SelfTargetMSIS can be estimated by the hardness of MSIS. However, we point out that in Dilithium, the estimation of SelfTargetMSIS was problematic: the method used by the authors cannot turn the assumption into MSIS. We further show that rather than solving MSIS, solving SelfTargetMSIS can only be turned into solving a variant of MISIS, we call it sel-MISIS in this paper, and the hardness of solving sel-MISIS is incomparable, if not simpler, than solving MSIS. We then give an algorithm for solving selMISIS called mul-ISIS-solver, which leads to a rough security estimation for Dilithium that maintains the parameters chosen by the authors, so there is no need to modify current implementations. However, we also point out that the hardness of sel-MISIS needs to be further studied to avoid potential attacks.

Keywords: Lattice-based cryptography, short integer solution problem, security estimation,

digital signature

Let me know; I'll forward you the paper/rubric/etc if you're interested.

--Daniel