From: Dang, Quynh H. (Fed)
To: Cooper, David (Fed); internal-pqc
Subject: Re: Hi all and Dustin,
Date: Tuesday, March 1, 2022 9:49:42 AM

Hi Dave,

I think it would be good if we cite the paper. The paper presents "best results" for Dilithium and Falcon that we have at this point on FPGA.

They worked hard to provide more and better data for Dilithium and Falcon to support our decision makings on time.

I don't think our report will be published very soon.

Quynh.

From: Cooper, David A. (Fed) <david.cooper@nist.gov>
Sent: Tuesday, March 1, 2022 9:22 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Hi all and Dustin,

Hi Quynh,

Do you think we need to cite this paper somewhere (even though it is coming in very late)? We already cite https://eprint.iacr.org/2021/1451, presenting a hardware implementation of Dilithium, from these same authors, and we also cite https://eprint.iacr.org/2021/662, which shows that Falcon verification is faster than Dilithium verification and that it uses fewer resources (smaller code and less RAM).

On 3/1/22 6:09 AM, Dang, Quynh H. (Fed) wrote:

> GMU just sent me a new paper for their high speed implementations of Dilithium (all operations) and verify function of Falcon
> here: https://eprint.iacr.org/2022/217.pdf
>
> Table V shows that Falcon's verify is resource efficient. And, Table VII shows that it is also very fast.
>
> Quynh.
>
> High-Performance Hardware Implementation of Lattice-Based Digital Signatures
>
> TABLE II: Dilithium parameters for version 3.1 at all sup-ported security

levels (2, 3, and 5). Parameter Value 2 3 5 q[modulus] 223 −213 + 1
d[dropped bit from t] 13
eprint.iacr.org