From: Dang, Quynh H. (Fed)
To: Cooper, David (Fed)
Subject: Re: how many cycles to compare with a byte in cost.
Date: Thursday, October 21, 2021 5:41:29 AM

Thank you David.

Quynh.

From: Cooper, David A. (Fed) <david.cooper@nist.gov>
Sent: Wednesday, October 20, 2021 3:09 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Subject: Re: how many cycles to compare with a byte in cost.

Hi Quynh,

It seems that I used 2000 cycles/byte in https://nistgov.sharepoint.com/sites/PQC/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FPQC%2FShared%20Documents%2FRound%202%20Presentations%2FPQC%20KEM%20Benchmarks%2020200407%2Epdf&parent=%2Fsites%2FPQC%2FShared%20Documents%2FRound%202%20Presentations.

In https://nistgov.sharepoint.com/sites/PQC/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FPQC%2FShared%20Documents%2FRound%202%20Presentations%2FPQC%20use%20in%20Protocols%2Epdf&parent=%2Fsites%2FPQC%2FShared%20Documents%2FRound%202%20Presentations, however, I noted that anywhere from 1000 to 6000 cycles per byte could be reasonable, depending on the processor and network being used.

In an email to the pqc-forum (https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/mvJy7vFPqfE), I presented examples using both 1000 cycles/byte and 2000 cycles/byte. Rainer Urian commented that some smart cards have relatively slow processors but very fast communications interfaces, so I followed up with an example using 85 cycles/byte.

On 10/20/21 2:24 PM, Dang, Quynh H. (Fed) wrote:

> Hi David,
>
> Could you remind me the number of cpu cycles you used to compare with the cost of sending 1 byte over the internet ?
>
> Thank you,
> Quynh.