From: Greg Zaverucha <gregz@microsoft.com>
Sent: Monday, July 29, 2019 7:41 PM
To: pqc-comments; pqc-forum
Subject: OFFICIAL COMMENT: Updates to Picnic implementations

Dear pqc-forum
We've updated the Picnic git repositories [1,2] with bug fixes and performance improvements for the Picnic2 parameter sets. One of the bug fixes causes the test vectors to change, so the latest code does not interoperate with the Round 2 submission package. We've also updated the design document [3], which fixes some typos.

Greg Zaverucha, on behalf of the Picnic team

[1] https://github.com/Microsoft/Picnic
[2] https://github.com/IAIK/Picnic.git
[3] https://github.com/microsoft/Picnic/blob/master/spec/design-v2.1.pdf

From: daniel.apon <daniel.apon@nist.gov>
Sent: Monday, July 29, 2019 9:23 PM
To: pqc-forum
Cc: pqc-comments
Subject: Re: OFFICIAL COMMENT: Updates to Picnic implementations

Hi Greg / Picnic team,

"We've updated the Picnic git repositories [1,2] with ... performance improvements for the Picnic2 parameter sets."

Would you please post (here, on the pqc-forum) a brief summary of the performance improvements you project from your recent changes?

Thank you kindly,
--Daniel, NIST PQC

On Monday, July 29, 2019 at 7:41:28 PM UTC-4, Greg Zaverucha wrote:

> Dear pqc-forum
>
> We've updated the Picnic git repositories [1,2] with bug fixes and performance improvements for the Picnic2 parameter sets. One of the bug fixes causes the test vectors to change, so the latest code does not interoperate with the Round 2 submission package. We've also updated the design document [3], which fixes some typos.
>
> Greg Zaverucha, on behalf of the Picnic team
>
> [1] https://github.com/Microsoft/Picnic
>
> [2] https://github.com/IAIK/Picnic.git
>
> [3] https://github.com/microsoft/Picnic/blob/master/spec/design-v2.1.pdf

From: 'Greg Zaverucha' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 30, 2019 5:13 PM
To: Apon, Daniel C. (Fed)
Cc: pqc-forum
Subject: RE: [pqc-forum] Re: OFFICIAL COMMENT: Updates to Picnic implementations

Hi Daniel
With yesterday's release, on an x64 system with AVX2 we expect a 1.4x to 1.5x speed-up for sign and verify. Memory usage for signing is reduced by about 3.2x to 3.5x and for verification is reduced by about 22x to 47x. The updated code has also been submitted to SUPERCOP. Improving the performance of the Picnic2 parameter sets (Picnic2-L1-FS, Picnic2-L3-FS, and Picnic2-L5-FS) is ongoing and once we're done we plan to update our design document with detailed benchmarks.

Greg

From: 'daniel.apon' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Monday, July 29, 2019 6:23 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: pqc-comments@nist.gov
Subject: [pqc-forum] Re: OFFICIAL COMMENT: Updates to Picnic implementations

Hi Greg / Picnic team,

"We've updated the Picnic git repositories [1,2] with ... performance improvements for the Picnic2 parameter sets."

Would you please post (here, on the pqc-forum) a brief summary of the performance improvements you project from your recent changes?

Thank you kindly,
--Daniel, NIST PQC

On Monday, July 29, 2019 at 7:41:28 PM UTC-4, Greg Zaverucha wrote:

> Dear pqc-forum
>
> We've updated the Picnic git repositories [1,2] with bug fixes and performance improvements for the Picnic2 parameter sets. One of the bug fixes causes the test vectors to change, so the latest code does not interoperate with the Round 2 submission package. We've also updated the design document [3], which fixes some typos.
>
> Greg Zaverucha, on behalf of the Picnic team