**From:** Patrick Longa <plonga@microsoft.com> via pqc-forum <pqc-forum@list.nist.gov>
**To:** pqc-forum@list.nist.gov
**Subject:** [pqc-forum] New results for SIKE
**Date:** Tuesday, March 22, 2022 01:52:09 PM ET

Dear NIST and pqc-forum,

I'm happy to share new results that show a significant speed up in the computation of SIKE.

The paper https://eprint.iacr.org/2022/367 presents algorithms that generalize interleaved Montgomery multiplications to the computation of extension field multiplications. This, in a more general sense, has implications for any scheme whose underlying arithmetic runs over an extension field GF(p^k) of large prime characteristic (e.g., it directly impacts all the recently proposed supersingular isogeny-based protocols like B-SIDH and SQISign, and also bilinear pairings).

Specifically for SIKE, our software implementation is sped up by approximately 1.3x (p434, level 1), 1.2x (p503, level 2) and 1.1x (p610, level 3). The alternative parameter p377 proposed in https://eprint.iacr.org/2020/1457 is also sped up by approximately 1.3x.

The new algorithms are already integrated to the SIDH library: https://github.com/microsoft/PQCrypto-SIDH

All these results correspond to a software implementation on a standard x64 computer. However, the algorithms are generic and are expected to benefit implementations on other platforms, including hardware, constrained devices, vectorized implementations, etc. (see the discussion in Section 6 of https://eprint.iacr.org/2022/367).

Kind regards,

Patrick

**From:** Bo Lin <bolinsco@gmail.com> via pqc-forum@list.nist.gov
**To:** pqc-forum <pqc-forum@list.nist.gov>
**CC:** Patrick Longa <plonga@microsoft.com>
**Subject:** [pqc-forum] Re: New results for SIKE
**Date:** Tuesday, April 12, 2022 08:49:59 AM ET

Hi, everyone,

Hope you're well!

This is a very interesting thread on SIKE and performance.
I have one comment on the SIKE performance in this discussion: the cost of big-number arithmetic accelerators for SIKE/SIDH or any other big-number arithmetic based schemes, such as RSA and ECC, is extremely low - everyone has a couple of them in their pockets, i.e., the free-of-charge credit cards. The absolute performance of this kind of schemes largely depends on the semiconductor technology. Actually, a simple presentation of the algorithms for low cost silicon design should also be considered. It can be imagined if SIKE is accepted as an NIST standard, micro-coded algorithms with mature hardware big-number accelerators will be a performance solution.

The performance comparison between Kyber and SIKE, as discussed in this thread, is interesting, but they may just find their favoured applications depending on application restrictions - some require high performance but loose key size while other may restrict on key size with tolerance on performance.

Regards,

Bo

On Tuesday, March 22, 2022 at 5:51:41 PM UTC Patrick Longa wrote:

> Dear NIST and pqc-forum,
>
> I’m happy to share new results that show a significant speed up in the computation of SIKE.
>
> The paper https://eprint.iacr.org/2022/367 presents algorithms that generalize interleaved Montgomery multiplications to the computation of extension field multiplications. This, in a more general sense, has implications for any scheme whose underlying arithmetic runs over an extension field GF(p^k) of large prime characteristic (e.g., it directly impacts all the

> recently proposed supersingular isogeny-based protocols like B-SIDH and SQISign, and also bilinear pairings).
>
> Specifically for SIKE, our software implementation is sped up by approximately 1.3x (p434, level 1), 1.2x (p503, level 2) and 1.1x (p610, level 3). The alternative parameter p377 proposed in https://eprint.iacr.org/2020/1457 is also sped up by approximately 1.3x.
>
> The new algorithms are already integrated to the SIDH library: https://github.com/microsoft/PQCrypto-SIDH
>
> All these results correspond to a software implementation on a standard x64 computer. However, the algorithms are generic and are expected to benefit implementations on other platforms, including hardware, constrained devices, vectorized implementations, etc. (see the discussion in Section 6 of https://eprint.iacr.org/2022/367).
>
> Kind regards,
>
> Patrick