**From:** Gilles Van Assche <gilles-pqc@noekeon.org> via pqc-forum <pqc-forum@list.nist.gov>
**To:** pqc-forum@list.nist.gov
**Subject:** [pqc-forum] Reduced-round Keccak for PQ schemes
**Date:** Friday, July 08, 2022 12:31:02 PM ET

Dear all,

First of all, we would like to congratulate the different teams whose algorithms are selected for standardization or for the 4th round!

Owing to the discussion initiated by John Mattsson in the thread "90s" version parameter sets, there is a need to optimize and simplify the use of symmetric primitives in the post-quantum schemes. We have understood that the calls to SHA-3/SHAKE/Keccak, e.g., to generate pseudo-random values, but also for other purposes, take a significant part of the total execution time in some of these schemes.

As its designer, we believe that Keccak is a future-proof and efficient primitive, among others when protections against side-channel attacks are required, but we also believe that its full 24 rounds are overkill. There has been sustained cryptanalysis on Keccak over the years and an amazing number of publications on this subject by the crypto community since its submission, and this gives a rather clear view of its safety margin [1]. Therefore, we would suggest to consider replacing Keccak-f[1600] with Keccak-p[1600, 12 rounds] in the definition of the standardized post-quantum schemes. Note that the Keccak-p[1600, 12 rounds] permutation is well defined in FIPS 202.

We think this would not change the safety margin of the post-quantum schemes in a significant way, yet give them a great speed-up and therefore yield a better performance-security trade-off for everyone.

Kind regards,
Gilles, Guido, Joan and Michaël

[1] https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fkeccak.team%2Fthird_party.html&data=05%7C01%7Cyi-kai.liu%40nist.gov%7C9a7d6491956847627bc408da60ff3e6d%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637928946627599796%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=Df6khttHy%2B0lT%2Fv8H6QiR4ZSNVpew9QoAMvldYbbtq0%3D&reserved=0 (note: some recent papers still have to be added)

--

**From:** John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
**To:** Gilles Van Assche <gilles-pqc@noekeon.org>, pqc-forum@list.nist.gov
**Subject:** Re: [pqc-forum] Reduced-round Keccak for PQ schemes
**Date:** Sunday, July 10, 2022 01:51:37 AM ET

Hi,

I think that is an interesting suggestion. My understanding is that Keccak-p[1600, 12] is twice as fast as Keccak-f[1600]. For the XOF maybe even Keccak-p[1600, 12] is overkill:

"The choice of SHAKE-128 as instantiation of the XOF is actually important for performance; also we do not need any of the traditional security properties of hash functions from SHAKE-128, but rather that the output “looks uniformly random.""

XOF, H, G, PRF, KDF could potentially use different amount of rounds. Could also consider using parallel hashing if any of the field are big enouhg to justify that.

I think ARM and RISC-V should be applauded for adding Keccak accelaration. My understanding is that the Keccak acceleration in these instuction set are quite general and would be equally good at accelerating Keccak-p[1600, 12 rounds].

I think the most relevant benchmark for PQC should be such a modern platform with ability to accelerate any Keccak variant. The PQC algorithms will likely be with us for many decades. I don't think it is a good idea to optimize for what is on the market today.

Cheers,

John

---

**From:** 'Gilles Van Assche' via pqc-forum <pqc-forum@list.nist.gov>
**Date:** Friday, 8 July 2022 at 18:31
**To:** pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
**Subject:** [pqc-forum] Reduced-round Keccak for PQ schemes

Dear all,

First of all, we would like to congratulate the different teams whose algorithms are selected for standardization or for the 4th round!

Owing to the discussion initiated by John Mattsson in the thread "90s" version parameter sets, there is a need to optimize and simplify the use of symmetric primitives in the post-quantum schemes. We have understood that the calls to SHA-3/SHAKE/Keccak, e.g., to generate pseudo-random values, but also for other purposes, take a significant part of the total execution time in some of these schemes.

As its designer, we believe that Keccak is a future-proof and efficient primitive, among others when protections against side-channel attacks are required, but we also believe that its full 24 rounds are overkill. There has been sustained cryptanalysis on Keccak over the years and an amazing number of publications on this subject by the crypto community since its submission, and this gives a rather clear view of its safety margin [1]. Therefore, we would suggest to consider replacing Keccak-f[1600] with Keccak-p[1600, 12 rounds] in the definition of the standardized post-quantum schemes. Note that the Keccak-p[1600, 12 rounds] permutation is well defined in FIPS 202.

We think this would not change the safety margin of the post-quantum schemes in a significant way, yet give them a great speed-up and therefore yield a better performance-security trade-off for everyone.

Kind regards,
Gilles, Guido, Joan and Michaël

[1] https://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-4efe772b67ea5506&q=1&e=7f83e25c-f3a7-49b1-9a3c-bd312753eea0&u=https%3A%2F%2Fkeccak.team%2Fthird_party.html (note: some recent papers still
have to be added)

--

f3a7-49b1-9a3c-bd312753eea0&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2Feae84996-8682-5345-ee41-ad0c2b52e10e%2540noekeon.org.