Kerman, Sara J. (Fed)

From: Philip Lafrance <Philip.Lafrance@isara.com>
Sent: Wednesday, January 10, 2018 11:47 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Gravity-SPHINCS

Dear Gravity-SPHINCS authors,

It appears that in your specification, Sections 2.3.3 through 2.3.6 describe the vanilla (plain, original) version of the Winternitz OTS scheme, but the bibliography references Hülsing et. al's WOTS+ paper; which is a major improvement on the vanilla scheme. I have not looked through the provided implementations to see which scheme they employ, but my personal recommendation would be to indeed use WOTS+; I suspect many on the forum would agree with that position.

It is possible that this has already been considered by you good folks, but I thought it worthwhile enough to bring up just in case. My apologies if this has been addressed elsewhere.

Warm regards,

Philip Lafrance

From: Guillaume Endignoux <guillaume.endignoux@gmail.com>
Sent: Thursday, January 11, 2018 6:41 PM
To: Philip Lafrance
Cc: pqc-comments; pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Gravity-SPHINCS

Dear Philip,

Thank you for your comments. We indeed did not give many details about this choice in the specification PDF, in order to keep it small. We give more details in [1, section 3.4], but here is a brief summary.

The rationale for WOTS+ [2] compared to WOTS was mostly to reduce the security to a second-preimage-resistant hash function instead of a collision-resistant function. However, the WOTS+ paper was written in a classical context, as it assumed second-preimage search in O(2^n) [2, section 3.3] when collision search was assumed to be in O(2^{n/2}). As expected, this allows to reduce signature size by 50% [2, section 5], since the hash output size n can be twice smaller than for WOTS. I might have missed something but this is the major selling point of WOTS+.

However, things are quite different against quantum attackers, as Grover's algorithm allows to search second preimages in O(2^{n/2}). We are not aware of a collision search algorithm with a better complexity than O(2^{n/2}), assuming that all costs are taken into account (not only time but also hardware, memory access, communication).

In the post-quantum context, we therefore think that the XOR masks added in WOTS+ compared to WOTS are an unnecessary complexity. This makes the proof as well as the implementation more complex (which means more risks of implementation bugs or potential flaws in the proofs), but without providing a significant security benefit.
The security proof of WOTS+ in [2, section 3.2] is quite long and non-trivial to follow, whereas the security proof of WOTS is simpler. You can find security proofs relevant to Gravity-SPHINCS in [3, chapter 6].

I hope that this helps answering your concern.

Best regards,
Guillaume Endignoux

[1] https://eprint.iacr.org/2017/933
[2] Hülsing, A.: W-OTS+ - shorter signatures for hash-based signature schemes. In: Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings. pp. 173–188 (2013)
[3] https://gendignoux.com/assets/pdf/2017-07-master-thesis-endignoux-report.pdf

Le 11 janv. 2018 16:35, "Philip Lafrance" <philip.lafrance92@gmail.com> a écrit :

> Dear Gravity-SPHINCS authors,
>
> It appears that in your specification, Sections 2.3.3 through 2.3.6 describe the vanilla (plain, original) version of the Winternitz OTS scheme, but the bibliography references Hülsing et. al's WOTS+ paper; which is a major improvement on the vanilla scheme. I have not looked through the provided implementations to see which