From: A. Huelsing <ietf@huelsing.net>
Sent: Thursday, September 26, 2019 3:44 AM
To: pqc-comments
Cc: pqc-forum; contact@sphincs.org
Subject: ROUND 2 OFFICIAL COMMENT: SPHINCS+

Hi everyone,

As promised, the SPHINCS+ team published two papers that establish a tight security reduction for SPHINCS+ without making use of the statistical assumption that was criticized on this forum before. Moreover, we give a detailed comparison to SPHINCS-256, Gravity-SPHINCS, and Picnic, as well as benchmarks for an optimized implementation of all proposed SPHINCS+ instantiations. The papers are available online at https://sphincs.org/resources.html

The new benchmarks and the comparison can be found in

The SPHINCS+ Signature Framework.
Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, Peter Schwabe.
CCS 2019 (to appear)

All the schemes that we compared have different security levels and make different assumptions. As we assume that the other teams selected the most favorable instances for their scheme, we left those untouched and generated SPHINCS+ instantiations with a comparable security level and comparable assumptions for each scheme. To select the best parameters for SPHINCS+ we used a parameter-exploration sage script which can be found online at https://sphincs.org/software.html and might be of independent interest.

The new proof can be found in the above paper and additionally builds on

Decisional second-preimage resistance: When does SPR imply PRE?.
Daniel J. Bernstein, Andreas Hülsing.
Asiacrypt 2019 (to appear)

As part of the proof we now fully formalized the concept of tweakable hash functions that was already informally introduced in the specification. This concept allows to separate the security reduction of the actual hash-based signature scheme from the analysis of how internal nodes are computed and is also applicable to the stateful hash-based signature schemes like LMS and XMSS.
We formulate clear security requirements for tweakable hash functions such that people from the symmetric community can construct tweakable hash functions from scratch.

Otherwise, we dealt with the following issue:

The issue

In an official comment on 24th of May, 2018, Chris Peikert noted that our security reduction does not support the actual security of any of our instantiations. The reason was a statistical assumption that we made on the length preserving hash function F which essentially maps n-bit to n-bit strings.
The assumption made was that every n-bit string has at least one other colliding n-bit string under F, i.e., every domain element has at least one second preimage. As correctly noted by Chris, this assumption does not hold for random n-to-n-bit functions and consequently is unlikely to hold for SHA2, SHA3, or Haraka based hash functions.

Our new results

In the SPHINCS+ proof the assumption is used to argue that a preimage finder A for function F can be turned into a second preimage finder B = A(F(x)) that loses at most a factor 1/2 in success probability. The argument is simply that if there are always at least two preimages, even a computationally unbounded A will return a preimage x' != x with probability >= 1/2.
Without the above assumption, the identity function is an easy counter example.

In the paper on decisional second-preimage resistance (DSPR) we introduce the concept of DSPR which can replace the above assumption. Intuitively DSPR says that it is hard to do better than guessing when deciding if a given input to F has a second preimage. Stated otherwise: It is hard to reliably recognize inputs that do not have a second preimage. This turns out to be sufficient to fix the above argument for B. Among other results, the DSPR paper then also shows that generic quantum attacks against DSPR have at least the same complexity as generic (second-)preimage attacks.

The SPHINCS+ paper takes the concept of DSPR, defines it for tweakable hash functions and then applies it to get a tight security reduction for SPHINCS+.

Best wishes,

Andreas for the SPHINCS+ team