From: pqc-forum@list.nist.gov on behalf of Smith-Tone, Daniel <daniel-c.smith@louisville.edu>
Sent: Monday, July 17, 2023 10:51 AM
To: pqc-forum
Subject: [pqc-forum] OFFICIAL COMMENT: 3WISE

Hello, Community,

There are some issues with the security claims of 3WISE, one of the newly submitted signature schemes to NIST's post-quantum standardization process. We have three observations that bring the security of all parameters well below their targeted security levels. We have contacted the submitter with these observations and the submitter agrees that the scheme is insecure, but prefers to not withdraw in the hope that studying the scheme will advance cryptanalysis.

First, the parameters are set in such a way that brute force search costs roughly 2^131 gates for security level 1, instead of 2^143 as is required in the CFP. This seems to be a simple mistake in reading the CFP and could be repaired by simply making the parameters a bit larger.

The second observation is that for the specific parameters, the prime q=17 is used. Then the inverse of the univariate map x|->x^3 is x|->x^11. Since the inverse function is isomorphic (in the isomorphism of polynomials sense) to the coordinatewise map raising the input the the power of 11, the entire function is a multivariate polynomial of total degree bounded by 11. By polynomial interpolation the inverse can be recovered by generating many input output pairs to the public key. The complexity of this task is far less than the claimed security levels, so this observation significantly breaks the scheme. The scheme could still be repaired from this attack by choosing a larger q such that 3^-1 mod q-1 is larger.

The third observation is that we may consider every public polynomial as a 3-tensor and by specializing every 3-tensor at some fixed but arbitrary vector input we recover a system of 2-tensors that has many rank 1 2-tensors in its span. Applying standard MinRank techniques recovers these maps. This analysis reveals equivalent output and input transformations.

The MinRank attack fully and practically breaks 3WISE. We have a script that breaks all 3WISE parameters in less than 30 seconds. For security level 1 parameters, the attack takes on average about 1.2 seconds.

An eprint describing the details of these observations will appear soon.

Cheers,
Daniel Smith-Tone