From: ilu...@ucm.es <iluengo@ucm.es> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] New version of DME for signature and KEM
Date: Monday, November 28, 2022 08:05:56 AM ET
Attachments: tabla.png

We have published the preprint "DME: a full encryption, signature and KEM multivariate public key cryptosystem" on https://eprint.iacr.org/2022/1538.

In the preprint, we describe a new version of the multivariate public key cryptosystem DME that was presented to the NIST PQC competition. DME is based on the composition of linear and exponential maps that allow the polynomials of the public key to be of a very high degree. This new version of DME adds one or two extra rounds of exponentials to the original two rounds and works over only two fields (F_q, F_q^2, q=2^e) instead of three. We get a huge reduction of the number monomials by imposing some carefully chosen linear conditions on the exponents, forcing many monomials to be equal after the last exponentials and their coefficienta to be combined into a single one. This "mixing" of the coefficients gives us a strong defense against structural cryptanalysis. For instance, in the 4 round scheme that we implemented, called DME-(4,8,2^64), the number of monomials of the components with reduction is (72,90,36,96) and without reduction (2^9, 2^9, 2^8, 2^9). The other new feature of DME is that the exponential matrices are now secret. The public key consist only of the final polynomials and given the (public) exponents of those polynomials there is a number of free parameter on the matrices that produces this public key. For instance, for the implemented DME-(4,8,2^64), for a single public key there are 2^84 sets of matrices that produce the same exponents, and gives amore security against structural attacks.

With this setting the composition gives a deterministic trapdoor one way permutation and allows use as random padding OAEP for KEM and PSS00 for signature. In the preprint, we provide SUPERCOP timings of DME-OAEP and DME-PSS00 for versions with three and four exponentials

and compare them with NIST finalists. For NIST security level 5, the size of ciphertext and signature is only 64 bytes.

The code of the reference implementation of DME-(3,8,2^64) and DME-(4,8,2^64) can be downloaded from https://github.com/miguelmarco/DME2, or from our website https://gauss.mat.ucm.es/dme/

Here are the timings and sizes for signature given in the preprint.

	NSL	KeyGen	Sign	Verify	PKey	Skey	Signature
dme-4r-8v-64b-pss	5	4609827	222307	55484	4843	675	64
dme-3r-8v-64b-pss	5	1953078	182009	40197	2793	542	64
dilithium2	2	169935	238597	147235	1312	2544	2420
dilithium5	5	319828	617804	337222	2492	4880	4595
falcon1024dyn	5	78644060	2080846	310257	1793	2305	1330
sphincsf256shake256robust	5	23130618	530274683	25373313	64	128	49216

FIGURE 1. Average CPU cycles for SIGN as measured by SuperCop on an Intel(R) Core(TM) i7-1165G7 @ 2.80GHz (message length = 93 bytes)

--