From: pqc-forum@list.nist.gov on behalf of kondo takeshi <kondotakeshi8@gmail.com>
Sent: Tuesday, April 30, 2024 9:27 AM
To: pqc-forum
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: MAYO

Dear all,

Recently I found the following result:
An improvement of algorithms to solve under-defined systems of multivariate quadratic equations by Prof. Hashimoto (available at https://doi.org/10.14495/jsiaml.15.53).

The article shows that there are three parameters in four parameters that need to be adjusted for the MAYO due to the impact of Prof. Hashimoto's algorithm.

I would like to ask if MAYO has provided new parameters based on the new analysis of Hashimoto's result and the corresponding implementation?
Or where can I find more information of the new parameters of MAYO?

all the best,
Kondo Takeshi
--

From: pqc-forum@list.nist.gov on behalf of Ward Beullens <Ward@beullens.com>
Sent: Thursday, May 2, 2024 2:26 PM
To: pqc-forum
Cc: kondo takeshi
Subject: [pqc-forum] Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: MAYO

Dear Kondo Takeshi, Dear all,

We are aware of the work of Professor Hashimoto. His work gives an improved method for finding a solution to a system of underdetermined multivariate quadratic systems (i.e. systems with more variables than equations). This is relevant for many schemes in the on-ramp competition, including MAYO.

When applied to the MAYO parameter sets, the latest technique of Hashimoto reduces the cost of forging a signature via a direct algebraic attack by between 14 bits (for MAYO1) and 2 bits (for MAYO2). The attack is completely generic in the sense that it does not exploit the structure of a MAYO system of equations, except for the fact that the system is underdetermined.

The most commonly used cost model in the MQ literature counts the number of field multiplications and multiplies this by the number of bit operations per multiplication to estimate the cost of the attack, ignoring everything that is not a multiplication, and ignoring the cost of (accessing) memory. In this cost model, the new attack has a slightly lower bit cost than attacks against AES-128/192/256 (see below). However, as explained in the MAYO submission document, we believe this is a very conservative cost model, and therefore a precise comparison against the bit-cost of an attack against AES-128/192/256 which accounts for all the operations, does not require a lot of memory and which parallelizes perfectly does not make a lot of sense. Nevertheless, the numbers are as follows:

Security Level 1
AES-128: 2^143
MAYO1: 2^131
MAYO2: 2^156

Security Level 3
AES-192: 2^207
MAYO3: 2^199

Security Level 5
AES-256: 2^272
MAYO5: 2^268

We believe that our MAYO parameters still satisfy the required security levels, in the sense that attacks on MAYO will be more costly (in “practical” terms such as dollar cost vs runtime) than corresponding attacks against AES.

Nevertheless, we observe that it would be relatively cheap to tweak the parameters so that the simple bit-cost lower bound for attacking MAYO again exceeds that of attacking AES, and we will do so if MAYO proceeds to the next round. We are also working on improving the attack, and we will set parameters to protect against what we deem to be plausible further improvements to Hashimoto's method. We expect this will have a limited impact on the key and signature sizes. E.g. ~20% increase for MAYO1, no impact for MAYO2, and smaller signatures but larger keys for MAYO3 and MAYO5.

The Mayo Team