From: 'VASSEUR Valentin' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Saturday, July 29, 2023 4:15 AM
To: pqc-comments
Cc: pqc-forum; thomas.debris@inria.fr; pierre.loisel@inria.fr
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: Enhanced pqsigRM

Dear enhanced pqsigRM team,

We have found substantial vulnerabilities in enhanced pqsigRM.

Enhanced pqsigRM is a hash and sign scheme which belongs to the family of GPV-like signatures but using error correcting codes instead of lattices.
In this framework it is crucial for the security to ensure that the signature distribution is independent from the secret key.
It turns out that we found significant biases in signatures distribution of enhanced pqsigRM that provide information on the secret key.

We have developed two scripts, available at <https://github.com/vvasseur/pqsigRM>.
The first script is designed for rapid execution and effectively illustrates the biases in the signature distribution.
The second script, although more time-consuming, leverages these biases to reveal the (U|U+V) structure of the secret key.

An ePrint providing more details will be made available soon.

The public key is constructed from a (U|U+V) code, to which rows are appended and then the columns are permuted.
More specifically, the public code admits a basis of the following form

(A, B)
(U, U) * P
(0, V)

where the matrices A, B, U, V and the permutation P are part of the secret key.
In this setup, U and V denote bases of codes of length 4096, while A and B possess a dimension of 2 and a length of 4096.
It is essential for security that both the structure and the permutation are kept secret.

In the absence of any rejection sampling in the (U|U+V) decoder, noticeable correlations can be observed between pairs of signature bits that are exactly 4096 indices apart.
Through the accumulation of approximately 100k signatures, it is easy to identify all pairs that correspond post-permutation, given that these pairs were positioned 4096 places apart pre-permutation in the private basis.
We call such pairs matched pairs.
Each post-permutation matched pair corresponds either to (i, i+4096) or (i+4096, i) pre-permutation.

As outlined by the authors of enhanced pqsigRM (see for instance Theorem 1 of the submission), signatures have to be distributed independently of the secret key (like in GPV schemes) and particularly signatures distribution has to be independent of P.
The above correlations over matched pairs show that it is not true.

Now if one wants to use these correlations to recover the secret key the primary goal is to discern between two cases among the matched pairs ((i, i+4096) or (i+4096, i) pre-permutation) to expose the (U|U+V) structure of the code.

This can be achieved by applying linear algebra to the generator matrix (rows of this matrix form a basis of the code) derived from the public key, using the matched pairs information.
First, one rearranges the columns of the public generator matrix such that the matched pairs are 4096 places apart.
We can accomplish this by successively filling a new matrix composed of two blocks, the left one and the right one.
For each matched pair (a, b) the column at position a goes on the left, and the column at position b on the right.

At this point, and setting aside the appended rows momentarily, we have a matrix that follows the form:

(π(U), π(U))
(π(V'), π(V''))

Here, π is a permutation and V' + V'' equates to V, they partition the columns of V into two parts.

Now, computing the product:

(π(U), π(U)) * (I, 0)
(π(V'), π(V''))   (I, I)

Yields the following result:

(0 , π(U))
(π(V), π(V''))

This allows us to identify π(U) and π(V) through straightforward Gaussian elimination.

A permutation rendering V'' as zero can be determined by leveraging the fact that swapping two matched columns followed by Gaussian elimination constitutes a linear operation.
This allows us to identify the necessary permutation by solving a set of linear equations.
The presence of the appended rows does not introduce any notable complexities.
We have identified a heuristic method that performs well in this regard.
Eventually, we end up with the following configuration:

(π(A) π(B))
(π(U), π(U))
(0 , π(V))

The recursive nature of the code ensures the detection of similar leakages at the second level, by considering the bits showing the second highest degree of correlation among post-permutation matched pairs.
Since U and V are also (U|U+V) codes, the same process can be applied, thus revealing the structure of π(U) and π(V).
This procedure can be recursively applied to continue revealing further code structure.

Best regards,

Thomas Debris-Alazard, Pierre Loisel and Valentin Vasseur

--

From: 'Perlner, Ray A. (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Friday, September 29, 2023 3:34 PM
To: pqc-comments
Cc: pqc-forum
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: Enhanced pqsigRM
Attachments: Enhanced pqsigRM Attack Outline.pdf

Dear Enhanced pqsigRM team and community,

We have observed a number of weaknesses in the public key of pqsigRM that we believe will lead to a practical full key recovery attack. Most notably, there are a significant number of weight-8 codewords in the dual of the hull of the public key for pqsigRM, which can be used to recover sets of 4 columns in the public key corresponding to columns with the same index mod 2048 in the private key. From this, an additional observation concerning weight 128 codewords in the hull of the public key, and the known attacks of Minder Shokrollahi 2007, Chizov Borodin 2013, we expect that we can practically recover an equivalent private key that is structurally identical to the pqsigRM private key. More details about the attack and what we have experimentally confirmed so far are in the attached slides. (We ultimately plan to finish implementing our attack and publish on eprint.)

This attack differs from the previous attack announced on this forum by Debris-Alazard, Loisel, and Vasseur in that our attack does not require access to signatures produced by the honest signer, and therefore cannot be avoided via rejection sampling or other modifications to the signing procedure. We further note that our attack demonstrates that the modifications Enhanced pqsigRM makes to the underlying Reed-Muller code not only are ineffective at hiding the private code’s structure, but in fact make that structure significantly easier to detect.

Cheers,

Ray Perlner on behalf of

Pierre Briaud,
Maxime Bros,
Ray Perlner,
Daniel Smith-Tone
--