From: AE Louisy <louisy.ae@gmail.com>
Sent: Tuesday, August 21, 2018 12:02 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: DualModeMS

Dear DualModeMS team,

I have two questions concerning your scheme:

In order to obtain EUF-CMA security, a modification is made to the Inner Layer. This modification is based on adding an l-long bit string to the original digest to compute a new one. I was wondering what value of l is chosen for the three parameter sets given.

I also wanted to know how exactly the choice to make 2^delta trees instead of one changes the size of the public key. I understand that having several trees means that each root needs a tag to identify it, but that results in public key sizes still slightly smaller than the ones given in the supporting documentation.

Sincerely,

A-E. Louisy,

Student in cryptography at Versailles University

From: Jocelyn Ryckeghem <Jocelyn.Ryckeghem@lip6.fr>
Sent: Monday, September 10, 2018 9:49 AM
To: pqc-comments; AE Louisy
Cc: pqc-forum@list.nist.gov; Jean-Charles Faugere; Ludovic Perret
Subject: Re: [pqc-forum] OFFICIAL COMMENT: DualModeMS

Dear Louisy,

In DualModeMS, 2^delta is the number of Merkle trees. Each root is stored in the public key, so the size of the public key is 2^delta
SHA3 hash. Moreover, we add in the public key a seed of K bits (K is the level of security in bits). It is used to generate Z, a set of tau elements of GF(2^k).

So, the size of the public key is:
for K=128, 2^4 * 256 bits + 128 bits = 528 bytes.
for K=192, 2^5 * 384 bits + 192 bits = 1560 bytes.
for K=256, 2^5 * 512 bits + 256 bits = 2080 bytes.

In the specification, the size of the public for K=256 is noted as
2112 bytes. This is a typo, the true size is 2080 bytes.

About the EUF-CMA security of the Inner layer, our implementation does not propose this functionality. However, as also mentioned in the GeMSS specification, there is a standard technique that allows to obtain EUF-CMA security for the Inner layer. The length l of a random salt should be 128 bits (for the three parameter sets) since the number of signature requests is assumed limited to 2^64.

Best regards,
the DualModeMS team.

AE Louisy <louisy.ae@gmail.com> wrote:

> Dear DualModeMS team,
>
>
> I have two questions concerning your scheme:
>
> In order to obtain EUF-CMA security, a modification is made to the
> Inner Layer. This modification is based on adding an l-long bit string
> to the original digest to compute a new one. I was wondering what
> value of l is chosen for the three parameter sets given.
>