
From: Ward Beullens <ward.beullens@student.kuleuven.be>
Sent: Monday, April 30, 2018 6:41 AM
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Gui

Dear all,

In my previous email I forgot to include the references, here they are:

- [1] Nicolas Courtois. Generic attacks and the security of quartz. In Public Key Cryptography, volume 2567 of Lecture Notes in Computer Science, pages 351–364. Springer, 2003.
[2] Van Oorschot, Paul C., and Michael J. Wiener. "Parallel collision search with cryptanalytic applications." *Journal of cryptology* 12.1 (1999): 1-28.

My apologies,
Ward

On 04/27/2018 04:11 PM, Ward Beullens wrote:

Dear all,

I believe there is a problem with the parameters of the Gui signature scheme for security level 1, and that a parameter change is needed.

The scheme uses a HFEv- trapdoor function which, with the proposed parameters for security level 1, outputs 168 bits. Given the limited number of output bits, this trapdoor cannot be straightforwardly used in a hash-and-sign scheme, because a collision attack would be able to forge signatures with roughly $2^{\lceil 168/2 \rceil} = 2^{84}$ evaluations of the trapdoor function. Instead, Gui uses the Feistel-Patarin construction [1], which requires k inversions of the trapdoor function to sign a message and k evaluations of the trapdoor function to verify a signature.

The paper [1] describes a generic attack on the Feistel-Patarin construction which requires roughly $2^{\lceil m*k/k+1 \rceil}$ evaluations of the trapdoor function (where m is the number of bits outputted by the trapdoor function), and requires roughly $m*2^{\lceil m*k/k+1 \rceil}$ bits of memory. For Gui this means 2^{112} evaluations of the public map, and $112*2^{112}$ bits of memory.

However, the distinguished point method of [2] can be used to have essentially the time complexity with roughly $3*112*2^{56}$ bits of memory (that is less than the amount of data that Google stores). I estimate that this attack requires 2^{135} (classical) gates, which is significantly less than the estimate of 2^{143} gates for a key-search on AES in the NIST call for proposals.

I think the best way to fix the problem is to increase the parameter k from 2 to 3 (the GeMSS submission has similar parameters and uses $k=4$). This would lead to a very modest increase of 32 bits in signature size, and a slowdown of the signing and verification algorithm of 50%.

I want to stress that this is a purely generic attack which only affects the security level 1 parameters, this does not indicate a weakness in the HFEv- construction.

Kind regards,
Ward

From: Bo-Yin Yang <moscito@gmail.com>
Sent: Thursday, June 14, 2018 9:33 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Gui

Dear Ward and everyone on this list,

We agree that we made a small mistake in our parameters and will change from $k=2$ to $k=3$ in Gui-184 in the future. This will not affect key sizes but will increase the signature by 32 bits as well as the runtime by 1.5x.

Best wishes
The Gui designers