From: panyanbin@amss.ac.cn
Sent: Wednesday, January 17, 2018 3:40 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: HQC

Dear Designers ans all,

We group find that the assumption that "DQCSD is hard" for the INDCPA security of HQC is not true over F_2. The similar attack were also proposed to attack the CPA security for the original NTRU, and by Castryck and Vercauteren to attack Giophantus(https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Giophantus-official-comment.pdf), and by Danilo to attack BIKE (https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/BIKE-official-comment.pdf). By the way, the assumptions over F_2 for BIKE suffer from the similar analysis.

Back to the assumption for HQC. Taking the public key of HQC as an example. To distinguish the public key (h,s=x+hy) with the uniformly random instance, where h is a uniformly random polynomial in R=F_2[x]/(x^n-1), x and y are two random polynomials in R with weight w, we evaluate the two polynomials h and s at 1.

Note that

s(1) = x(1)+h(1)y(1) mod 2, that is,

s(1) = w + wh(1) mod 2.

For the real public key pairs, the relation above always holds, but for a uniformly random instance (h,s), it just holds with probability 1/2.

So it seems not too hard to distinguish the real pk from the uniformly random instance by checking if the relation holds or not. The same idea can be extended to contradict the DQCSD assumption.

Moreover, IF we could find two message m_0 and m_1, such that (m_0G)(1) and (m_1G)(1) are different (mod 2), we can easily present an attack against the IND-CPA security, by the fact that v(1)= (mG)(1)+s(1)r_2(1)+e(1) and v(1), s(1), r_2(1), e(1) are known.

We have to point out that we can not recover the private key or recover the message without the private key by now. By employing some tricks, one may make the system provable security. Maybe an easy way to resist the attack above is to choose the short polynomial with dynamic weight instead of the fixed one. For example, we can choose x (or y, e,r_1, r_2) of weight w with probability 1/2, and of weight w-1 with probability 1/2.

If we miss something, please let us know.

Best regards,

Zhen Liu, Yanbin Pan

From: Misoczki, Rafael <rafael.misoczki@intel.com>
Sent: Thursday, January 18, 2018 11:25 AM
To: panyanbin@amss.ac.cn; pqc-comments
Cc: pqc-forum@list.nist.gov; Misoczki, Rafael
Subject: RE: [pqc-forum] OFFICIAL COMMENT: HQC

Dear Zhen Liu, Yanbin Pan,

The BIKE team would like to clarify (again) that the observation presented by Danilo does not represent an attack on our schemes.

In fact, this is simply a property of the scheme of which we were already aware. From a practical perspective, the adversary may observe the parity of the Hamming weight of the error, and learns nothing new because this weight is a public parameter of the scheme.

Thanks to Danilo's observation, however, we noticed a small imprecision in our proof: this is easy to fix and the correction will be posted in the BIKE web page at: www.bikesuite.org.

This fix does not change the hardness assumptions of the scheme and does not induce any change in the proposed BIKE parameter sets. It goes without saying that no change to the algorithms/spec of the scheme is needed either.

Best regards,
BIKE Team

From: panyanbin@amss.ac.cn [mailto:panyanbin@amss.ac.cn]
Sent: Wednesday, January 17, 2018 12:40 AM
To: pqc-comments@nist.gov
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: HQC

Dear Designers ans all,

We group find that the assumption that "DQCSD is hard" for the INDCPA security of HQC is not true over F_2. The similar attack were also proposed to attack the CPA security for the original NTRU, and by Castryck and Vercauteren to attack Giophantus(https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Giophantus-official-comment.pdf), and by Danilo to attack BIKE (https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/BIKE-official-comment.pdf). By the way, the assumptions over F_2 for BIKE suffer from the similar analysis.

Back to the assumption for HQC. Taking the public key of HQC as an example. To distinguish the public key (h,s=x+hy) with the uniformly random instance, where h is a uniformly random polynomial in R=F_2[x]/(x^n-1), x and y are two random polynomials in R with weight w, we evaluate the two polynomials h and s at 1.

From: Jean-Christophe Deneuville <jean-christophe.deneuville@unilim.fr>
Sent: Saturday, December 15, 2018 5:47 AM
To: panyanbin@amss.ac.cn; pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: HQC

Dear Pan Yanbin and all,

In the original specifications, we introduced the Decisional Syndrome Decoding problem for Quasi-Cyclic codes (aka. DQCSD).
We were made aware that a distinguisher could be obtained for this problem using the bit parity. We are grateful to Pan Yanbin and Ray Perlner for bringing to our knowledge the existence of such a distinguisher.

Similarly to the BIKE submission, we introduce a parity version of the DQCSD problem that allows to thwart the reported distinguisher.
Both the definitions of the problems and the security proof were updated. Namely we added a parity version of the DQCSD problem, which is similar to what was done for BIKE. In particular, the details appended vanish the attack presented in [1].

We stress that these changes do not impact on the practical security of the scheme. The reference implementation and the KATs remain unchanged.

The latest documentation is available on the official website: https://pqc-hqc.org/

Sincerely,
The HQC team

[1] Breaking the Hardness Assumption and IND-CPA Security of HQC Submitted to NIST PQC Project, Zhen Liu, Yanbin Pan, and Tianyuan Xie, CANS, LNCS 11124, pp. 344–356, 2018

On 17/01/2018 -- 09:39, panyanbin@amss.ac.cn wrote:

> Dear Designers ans all,
>
> We group find that the assumption that "DQCSD is hard" for the INDCPA security of HQC is not true over F_2. The similar attack were also proposed to attack the CPA security for the original NTRU, and by Castryck and Vercauteren to attack Giophantus(https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Giophantus-official-comment.pdf), and by Danilo to attack BIKE (https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/BIKE-official-comment.pdf). By the way, the assumptions over F_2 for BIKE suffer from the similar analysis.
>
> Back to the assumption for HQC. Taking the public key of HQC as an example. To distinguish the public key (h,s=x+hy) with the uniformly random instance, where h is a uniformly random polynomial in R=F_2[x]/(x^n-1), x and y are two random polynomials in R with weight w, we evaluate the two polynomials h and s at 1.