From: zhenfei <zzhang@onboardsecurity.com>
Sent: Tuesday, January 23, 2018 10:32 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: NTRUEncrypt
Attachments: signature.asc

Dear all,

We would like to thank Jingnan He and Xianhui Lu for pointing out a bug in our code.

In the discrete Gaussian sampling algorithm ntru-pke-1024/DGS.c

```
void DGS (     int64_t   *v,      /* output   vector */
const uint16_t  dim,     /* input    dimension */
const uint8_t   stdev)   /* input    standard deviation */,
```

where the stdev is 724 and therefore requires more than 8 bits to store.

We have fixed this bug. The updated code will be available at

https://www.onboardsecurity.com/nist-post-quantum-crypto-submission

Best regards,

The NTRU team