From: Lorenz Panny <l.s.panny@tue.nl>
Sent: Monday, December 25, 2017 5:03 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: RVB

Dear all,

the following sage script quickly computes the secret key from a given public key in the RVB submission:

https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fyx7.cc%2Ffiles%2Fchaos.sage.txt&data=02%7C01%7Csara.kerman%40nist.gov%7Cbd086f558c364b3f132b08d54b7eba7f%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C636497930025212178&sdata=D3mfSq4ylm69Ab7iz5%2BNDalHPPk4GjZCmjZtKH%2BIOZs%3D&reserved=0

The attack is essentially the algorithm of [0] except for using LLL to find k such that a+kb is close to an integer. The script successfully recovers the secret keys of all known-answer tests.

-- Lorenz

[0]
https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2Fcs%2F0411030&data=02%7C01%7Csara.kerman%40nist.gov%7Cbd086f558c364b3f132b08d54b7eba7f%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C636497930025212178&sdata=bBqFnxLcKlT9Zc9IKdqWR640WWWITJHqG3%2FQJjwes%2Bs%3D&reserved=0

From: Bernd Roellgen <roellgen@globaliptel.com>
Sent: Friday, January 05, 2018 11:07 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: RVB

Dear all, dear Mr. Panny,

using the Lenstra–Lenstra–Lovász (LLL) lattice basis reduction algorithm is something that we didn't have on our radar screen. It successfully breaks the entire encryption scheme in almost no time.
The attack is reproducible and well-documented. Congratulations for this great work!

This is a perfect example for the usefulness of such competitions and the objective peer review that goes along with it.

We officially withdraw our algorithm.

Thanks,

Bernd and Gilbert