From: Danilo Gligoroski <danilog@ntnu.no>
Sent: Saturday, December 30, 2017 6:35 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: LOCKER

Dear LOCKER designers,

It seems that LOCKER is suffering from a similar non-randomness as LAKE.

Example from LOCKER-I KAT file (a similar situation is with all variants of LOCKER) for count = 0 Parsing the ciphertext in chunks of 18 nibbles gives the following:

```
ct = {
"ACFF1884B5518CCC6C", "B488CB7E7A8FD17E12", "B488CB7E7A8FD17E12", \ "5CF175DF214B054568",
"B96A50B09CC6C8FD6E", "D15A4A342BA0B05F51", \ "68301A84B76678A23F", "F00E6D5B941A898904",
"8049A425ECA2AC9945", \ "DCB8D1FACDE9A9DC2D", "ACFF1884B5518CCC6C", "E879BEA15BC4D43B7A", \
"FDECF6957253900A78", "D15A4A342BA0B05F51", "C92D99CEE47EEDED2F", \ "159548342997443102",
"95DCEC11C535E8A847", "65D2814A512F612143", \ "000000000000000000", "2154276FBFBA39D655",
"0DE29BCEE64919837C", \ "E879BEA15BC4D43B7A", "D15A4A342BA0B05F51", "A11D834A5318954F10", \
"68301A84B76678A23F", "3923F495706464642B", "ACFF1884B5518CCC6C", \ "95DCEC11C535E8A847",
"0DE29BCEE64919837C", "B488CB7E7A8FD17E12", \ "0DE29BCEE64919837C", "ACFF1884B5518CCC6C",
"159548342997443102", \ "68301A84B76678A23F", "5CF175DF214B054568", "159548342997443102", \
"8049A425ECA2AC9945", "5CF175DF214B054568", "983E77DF237CF12B3B", \ "4486A625EE9558F716",
"F00E6D5B941A898904", "5113EE11C7021CC614", \ "000000000000000000", "ACFF1884B5518CCC6C",
"000000000000000000", \ "3923F495706464642B", "D15A4A342BA0B05F51", "2CB6BCA159F3205529", \
"E59B256FBD8DCDB806", "000000000000000000", "3923F495706464642B", \ "F00E6D5B941A898904",
"2CB6BCA159F3205529", "DCB8D1FACDE9A9DC2D", \ "65D2814A512F612143", "C92D99CEE47EEDED2F",
"8DAB3FEB0AEBB51A39", \ "49643DEB08DC41746A", "C4CF02000237F46E53", "5CF175DF214B054568", \
"7047C97E78B8251041", "68301A84B76678A23F", "C92D99CEE47EEDED2F", \ "4486A625EE9558F716",
"D15A4A342BA0B05F51", "49643DEB08DC41746A", \ "8DAB3FEB0AEBB51A39", "C92D99CEE47EEDED2F",
"E879BEA15BC4D43B7A", \ "5CF175DF214B054568", "2154276FBFBA39D655", "D15A4A342BA0B05F51", \
"FDECF6957253900A78", "8049A425ECA2AC9945", "B488CB7E7A8FD17E12", \ "A11D834A5318954F10",
"3923F495706464642B", "3923F495706464642B", \ "D15A4A342BA0B05F51", "65D2814A512F612143",
"3923F495706464642B", \ "ACFF1884B5518CCC6C", "D15A4A342BA0B05F51", "7ED536F670A3949568", \
"A5F7BD6AD16342AF1C", "7229AED2BF4CECB47B", "A0DF6B1F67779754FC", \ "D83E94073ED0D13B5C",
"1C35B9C24A29CFC0B8", "182AE2F974194E31D6", \ "0B319F990985CC5DC5", "326D52D69CC14F8148",
"B1AE7CA34DD769D81F", \ "684FD212AC23F6ECF7", "8F546C0ED3529537BB", "38DEC38FE0ACCA6475", \
"1B2390E788AD171BEB"}
```

and we can see that in the list of 97 sub-strings in ct, there are "only" 43 different sub-strings { "000000000000000000", "0B319F990985CC5DC5", "0DE29BCEE64919837C", \ "159548342997443102", "182AE2F974194E31D6", "1B2390E788AD171BEB", \ "1C35B9C24A29CFC0B8", "2154276FBFBA39D655", "2CB6BCA159F3205529", \ "326D52D69CC14F8148", "38DEC38FE0ACCA6475", "3923F495706464642B", \ "4486A625EE9558F716", "49643DEB08DC41746A", "5113EE11C7021CC614", \ "5CF175DF214B054568", "65D2814A512F612143", "68301A84B76678A23F", \ "684FD212AC23F6ECF7", "7047C97E78B8251041", "7229AED2BF4CECB47B", \ "7ED536F670A3949568", "8049A425ECA2AC9945", "8DAB3FEB0AEBB51A39", \ "8F546C0ED3529537BB", "95DCEC11C535E8A847", "983E77DF237CF12B3B", \ "A0DF6B1F67779754FC", "A11D834A5318954F10",

```
"A5F7BD6AD16342AF1C", \ "ACFF1884B5518CCC6C", "B1AE7CA34DD769D81F", "B488CB7E7A8FD17E12", \
"B96A50B09CC6C8FD6E", "C4CF02000237F46E53", "C92D99CEE47EEDED2F", \ "D15A4A342BA0B05F51",
"D83E94073ED0D13B5C", "DCB8D1FACDE9A9DC2D", \ "E59B256FBD8DCDB806", "E879BEA15BC4D43B7A",
"F00E6D5B941A898904", \ "FDECF6957253900A78"}
```

Since LOCKER offers an IND-CPA proof involving games G0, G1, G2 and G3, this non-randomness can seriously jeopardize the correctness of the proof.

Best regards,
Danilo!

From: Danilo Gligoroski <danilog@ntnu.no>
Sent: Sunday, January 07, 2018 6:30 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: LAKE

Dear LAKE and LOCKER designers,

I found the following 2 properties of your schemes that are not discussed in your documentation. For the sake of short presentation I will describe the procedures for LAKE, but the same properties hold for LOCKER too.

1. For a given pair (pk, sk) it is easy for everyone to produce millions of new equivalent public keys pk1, pk2, ... such that K = Decap(sk, Encap(pk)) = Decap(sk, Encap(pk1)) = Decap(sk, Encap(pk2)) = ... 2. For a given ciphertext c = e1 + e2 . h it is easy for everyone who captures c, to produce millions of equivalent ciphertexts c1, c2, ..., such that K = Decap(sk, c) = Decap(sk, c1) = Decap(sk, c2) = ...

The procedure for producing these equivalent public keys and ciphertexts is quite simple:

1. Let B^n be the n-dimensional vector space <0, 1>^n (which is a subspace of F^n_{2^m}) 2. Generate a random vector scrambler mod P \in B^n, such that scrambler is invertible mod P 3. Produce an equivalent pk1 = scrambler . pk or equivalent c1 = scrambler . c

The equivalent pk1 and c1 have the properties 1 and 2.

The correctness of the above procedure comes from a trivial property of B^n: For any vector space E, E . B^n = B^n . E = E.

In my opinion, the first property can be seen as an advantage of the scheme, since it gives some possibilities to anonymise the public key, but it is in conjunction with the second property. And the second property is quite unusual for a public key scheme, since it gives opportunity to the adversaries to scramble the ciphertext, but the decrypting party will not notice that. Maybe that is not a serious problem for an IND-CPA scheme, but still it is quite unusual for a public key scheme.

Best regards,
Danilo!

P.S. My guess is that similar properties hold for the patented scheme RQC, but once I read that it is patented I stop my analysis for it.