From: Yu Yu <yuyuathk@gmail.com>
Sent: Sunday, December 31, 2017 7:50 AM
To: Gaborit
Cc: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] A probable security issue for LEPTON

Dear Philippe,

Not aware of [1] before, so we just did a quick pass through [1]. We're a bit confused about statements in [1] like "we are interested in finding a lower bound on the cost", and indeed after giving a series of lower bounds it reaches the main theorem about the algorithm efficiency with precise constant factor in the exponent. Typically, we care about only the average-case or even the opposite (upper bounds) of the costs when analyzing the efficiency of algorithms. [1] is not self-contained either, and it simply revokes previous ISD solvers (for linear error rate which may not immediately apply to sublinear case). We will further investigate the issue and give more comments soon. Here're our responses to address the rest comments of yours:

1. the LEPTON proposal seems to claim novelty of their approach when our HQC paper [2] (under revision) publicly available on arxiv for more than one year (and not cited), proposes exactly the same protocol (the HQC proposal of the NIST call). Overall LEPTON seems to be strongly inspired of the uncited HQC paper [2], but with very weak and attackable proposed parameters for the NIST call and with potentially corrected parameters which would lead to probably strongly worse parameters than HQC.

We didn't know about your arxiv paper [2] (personally we just don't read papers from arxiv), and we will cite it in the next update of the documentation. However, please note that our basic CPA construction more resembles (and was inspired by) the Ring-LPN based PKE by Damgard and Park in 2012 (see Definition 2.24 of [3]): we even use the same Ring structure as in [3], i.e., for a trinomial g(x)=x^n+x^m+1 with small m. The difference to [3] is that we advocate the use of irreducible trinomial (justified by showing some connections between LPN and Ring-LPN) and we use a noise distribution of exact weight instead of an expected weight (the Bernoulli distribution). The use of such distribution dates back to Alekhnovich's original PKE, the exact LPN (Asiacrypt 2012) and the LSPN problem [6,7]. The use of BCH and repetition codes for error correcting in our proposal is very natural because they are simple and have relatively high performance, as far as we know several other proposals also use those ECC codes as building blocks. Furthermore, we would also like to claim some credits by having publications about LPN-based PKE [8] and the idea of "LPN with structured non-Bernoulli secret/noise" [9] at Crypto 2016 and Eurocrypt 2016.

Finally, we appreciate it if we all can keep the discussions technical and refrain from making hypothetical statements. As said above, our construction bears much more similarity to DP12 [3] than the one in [2]. If we had known of your work before, we wouldn't be bothered to add one more citation. Further, I don't think any IND-CPA (Ring-)LPN-based proposal should claim novelty about the protocol itself as all known ones are just following the blueprint of Alekhnovich [4] up to the choices of noise distributions, the structure of Rings, etc.

2. It is possible to find secure parameters with the approach proposed by LEPTON, but the fact that g(x) is not of the form x^n-1 and is a trinomial, implies at least a 50% increase of the error weight to correct, so that even potentially modified parameters will always lead far less interesting parameters than for the HQC proposal.

The reason that we don't use g(x)=x^n-1 (or any reducible polynomial over GF(2) in general) is due to the concern raised in [5,11] that certain attacks might gain advantages by possibly utilizing the factorization of the underlying polynomials over GF(2). We're not saying it's definitely an issue but we choose to avoid it by using (which we believe more conservative) irreducible trinomial, which incurs only some slightly more overheads than the g(x)=x^n-1 case.

Best regards and Happy New Year !

Yu Yu and Jiang Zhang

[1] Rodolfo Canto Torres, Nicolas Sendrier: Analysis of Information Set Decoding for a Sub-linear Error Weight. PQCrypto 2016: 144-161

[2] Carlos Aguilar, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Gilles Zémor (under revision), Efficient Encryption from Random Quasi-Cyclic Codes https://arxiv.org/abs/1612.05572

[3] Ivan Damgard and Sunoo Park. How Practical is Public-Key Encryption Based on LPN and Ring-LPN? https://eprint.iacr.org/2012/699

[4] Michael Alekhnovich. “More on Average Case vs Approximation Complexity”. In: FOCS 2003, pp. 298–307.

[5] Guo, Q., Johansson, T., Löndahl, C.: A new algorithm for solving ring-lpn with a reducible polynomial. IEEE Trans. Information Theory 61(11), 6204–6212 (2015)

[6]Grigorescu, E., Reyzin, L., Vempala, S.: On noise-tolerant learning of sparse parities and related problems. In: 22nd International Conference on Algorithmic Learning Theory (ALT 2011). pp. 413–424 (2011)

[7] Valiant, G.: Finding correlations in subquadratic time, with applications to learning parities and juntas. In: 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012). pp. 11–20 (2012), full version appeared at J. ACM 62(2), 13:1–13:45 (2015)

[8] Yu Yu, Jiang Zhang. "Cryptography with Auxiliary Input and Trapdoor from Constant-Noise LPN", Advances in Cryptology - CRYPTO 2016, pp.214-243.

[9] Yu Yu, John Steinberger. "Pseudorandom Functions in Almost Constant Depth from Low-Noise LPN", Advances in Cryptology - EUROCRYPT 2016, pp. 154-183.

[10] Yu Yu, Jiang Zhang. The Lepton proposal submitted to NIST.

[11] Stefan Heyse. Post Quantum Cryptography: Implementing Alternative Public Key Schemes on Embedded Devices. PhD thesis, Ruhr-University Bochum, 2013. https://www.emsec.rub.de/media/attachments/files/2014/03/thesis-stefan-heyse.pdf.

2017-12-30 3:54 GMT+08:00 Gaborit <gaborit@unilim.fr>:

> dear all,
>
> I think there may be a security issue with the LEPTON proposal,
> giving a security loss of a factor 3 or 4 on the security exponent,
> depending on the type parameters considered.
>
> In LEPTON the ind-CPA security of the
> system is reduced to solving the ring-CLPN problem (p.8).
> in fact the previous problem can be interpreted
> in term of a decoding problem :

From: Yu Yu <yuyuathk@gmail.com>
Sent: Wednesday, January 03, 2018 11:58 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Lepton

Dear all,

We are grateful to Dr. Philippe Gaborit for pointing out a more precise asymptotic estimate on the classical hardness of underlying LPN variant considered in our Lepton proposal. In particular, for sublinear error rate k/n=o(1) and coding rate R=1/3 the complexity should be O(n^3)*2^{1.75k}, where 1.75\approx 3*log(1/(1-R)) and factor O(n^3) accounts for the cost of Gaussian elimination and is often omitted. The implication is that we need to use larger values for k and n and re-evaluate the performance in the next update of the proposal. Looking back now, it seems that our implementation was too good (efficient) to be true (secure), i.e., half of the CPU cycles in encryption/decryption were spent on SHA-3 for randomness generation, so we are expecting something reasonably good when adjusted to larger parameters.

We stress our security reductions are not affected. Our original intention of using exact k-out-of-n distribution to replace rate (k/n)-Bernoulli in LPN was to facilitate noise sampling and to hopefully lift security (without giving formal proofs). Now we are convinced that the latter wishful claim is not true: our LPN variant is just as hard as standard LPN of the same noise rate (up to a constant factor in the exponent), just as we proved in Lemma 2 of the proposal.

Best regards,

The Lepton Team

From: gaborit <gaborit@unilim.fr>
Sent: Saturday, February 10, 2018 5:27 AM
To: pqc-comments
Subject: OFFICIAL COMMENT: Lepton

hi,

my orignal mail (12/29/2017), which permits to understand the LEPTON's team answer, I maintain
all which is explained the mail, in terms of size of parameters.

best,

philippe

%%%
%%%%%

From: Gaborit [mailto:gaborit@unilim.fr]
Sent: Friday, December 29, 2017 2:55 PM
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] A probable security issue for LEPTON

dear all,

I think there may be a security issue with the LEPTON proposal, giving a security loss of a factor 3 or 4 on the security exponent, depending on the type parameters considered.

In LEPTON the ind-CPA security of the
system is reduced to solving the ring-CLPN problem (p.8).
in fact the previous problem can be interpreted in term of a decoding problem :

solving the classic SD problem (with protocol notation p.9):

H.X^t=S

```
with H= (I 0 A)
        (0 I B)
```

X=(e1,e2,x)

and
S=(c1,c2)^t.

for A and B nxn matrices associated to the multiplication by a and b mod g(x) as explained in the proposal; for e1,e2 and x of average weight t=mu.n (defined in the proposal).

For low parametres of the range given in the proposal, the complexity of solving the pb given in [1] is 2^(1.75.t),for t=20,..40, which gives complexities of $2^{\wedge 35}$ to $2^{\wedge 70}$ when the paper announces security from 128 to 262 bits.
The previous attack can also be done directly on the key or on the message by considering not a 2n x 3n matrix as explained before, but a n x 2n matrix: [I, A] for instance. In that case the attack has a greater complexity in 2^(2t), so that the attack leads to complexities with only a factor 3 loss in the security exponent with previous choices of t=\mu.n.

Now two additional remarks.

1. the LEPTON proposal seems to claim novelty of their approach when our HQC paper [2] (under revision) publicly available on arxiv for more than one year (and not cited), proposes exactly the same protocol (the HQC proposal of the NIST call):

- same cyclic variation of the protocol based on Aleknovich's approach
- same non trivial choice of error correcting code

the only difference being that

- the LIPTON proposal considers an irreducible polynomial g(x) rather than g(x)=x^n-1 (which does not modify the security for n a primitive number mod 2)
- our error analysis is more precise and simulated.
- we rely on the adapted code-base problems (decoding QC codes) for this type of parameters rather than on almost equivalent LPN problem variations. All the attacks described in this note are described in [2].

2. It is possible to find secure parameters with the approach proposed by LEPTON, but the fact that g(x) is not of the form x^n-1 and is a trinomial, implies at least a 50% increase of the error weight to correct, so that even potentially modified parameters will always lead far less interesting parameters than for the HQC proposal. Overall LEPTON seems to be strongly inspired of the uncited HQC paper [2], but with very weak and attackable proposed parameters for the NIST call and with potentially corrected parameters which would lead to probably strongly worse parameters than HQC.

[1] Rodolfo Canto Torres, Nicolas Sendrier:
Analysis of Information Set Decoding for a Sub-linear Error Weight.
PQCrypto 2016: 144-161

[2] Efficient Encryption from Random Quasi-Cyclic Codes Carlos Aguilar, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Gilles Zémor (under revision), available since december 2016 at https://arxiv.org/abs/1612.05572

best,

philippe