**From:** D. J. Bernstein <djb@cr.yp.to>
**Sent:** Monday, April 30, 2018 3:45 AM
**To:** pqc-comments
**Cc:** pqc-forum@list.nist.gov
**Subject:** OFFICIAL COMMENT: GeMSS
**Attachments:** signature.asc

I'm writing to correct some misimpressions regarding asymptotic MQ security that are created by the GeMSS/DualModeMS presentation:

https://csrc.nist.gov/CSRC/media/Presentations/DualModeMS-GeMMS/images-media/DualMode-and-GeMMs-April2018.pdf

Specifically, page 15 of the PDF (slide "10/19") has the following summary of the costs of quantum versions of FXL stated in two independent papers for solving m equations in m variables over F_q:

* "O(2^0.462m)" from a "2017" paper (posted 2017.12.19).
* "When q=2, O(2^0.472m)" from a "PQC 2018" paper (posted 2017.12.15).

There are four specific issues here.

Issue #1: Because the "When q=2" restriction is stated only for the second number, readers will assume that the first number applies to larger fields---for example, that switching from F_2 to F_3 for the same m doesn't provide larger security at this level of detail.

That's wrong. The first number 0.46240... is also limited to F_2. For
F_3 the best exponent known is 0.70425..., below 0.5 lg 3 = 0.79248...
but above 0.46240..., analogously to the pre-quantum situation of F_3 having larger exponent than F_2. See the 2017.12.15 paper for details.
(The 2017.12.19 paper doesn't consider cases beyond F_2.)

Issue #2: Readers will assume that the 0.462 and 0.472 are the best exponents obtained in these two papers, and are likely to think that this discrepancy shows some instability in the understanding of this class of algorithms.

But that's also wrong. The two papers obtain the same exponent here. See Table 4.10 in the 2017.12.15 paper, "GroverXL operation-count exponent ... rounded down to multiple of 0.00001", top-left corner (top being F_2; left being the same number of equations as variables), "0.46240".
This is the same as the "0.462" exponent from the 2017.12.19 paper.

There's also a "0.47210" in the 2017.12.15 paper, but that's in a different metric, so it's wrong to juxtapose the numbers without mentioning that the metrics are different. Specifically:

* Exponent 0.46240...+o(1) is in a simplified operation-count metric.
  This metric is considered in both papers.

* Exponent 0.47210...+o(1) is in a realistic area-time metric. This
  metric is analyzed only in the 2017.12.15 paper, and this exponent
  isn't achieved by the algorithm outlined in the 2017.12.19 paper.

The gap here occurs for the same reasons as the long-established gap between analogous metrics for pre-quantum integer factorization: linear algebra uses a lot of communication.

Issue #3: The "0.462" and the "0.472" are the results of rounding the actual exponents down. This needs to be stated explicitly, for example with dots. The issue here isn't that this is a big quantitative gap; the issue is that careful readers comparing, e.g., "0.462" to "0.46240..."
are again being told that there's a discrepancy, which isn't true.

Issue #4: A o(1) in the exponent has disappeared in favor of an O() outside the formula. This isn't justified by either paper. This _could_ be a big quantitative gap compared to any reasonable O constant---one would have to do a more detailed analysis to tell.

Of course rounding _up_ can avoid the overt error: if the time is at most 2^((0.462...+o(1))m) then it's true that the time is at most, say, O(2^(0.463m)). However, careful readers comparing two of these slight asymptotic overestimates are again led to believe that there's a discrepancy when there actually isn't (unless the slight overestimates happen to coincide). Furthermore, the o(1) is useful as an alert regarding suppressed subexponential factors.

---Dan

P.S. I'm a coauthor of the 2017.12.15 paper and gave a talk on the paper at PQCrypto 2018. I was careful in the talk to point out the subset that was done independently (obtaining the same 0.46240... exponent) in the
2017.12.19 paper. I'm puzzled that the authors of the 2017.12.19 paper, overlapping the authors of these slides, have chosen to juxtapose 0.472 from "2018" with 0.462 from "2017" without mentioning that the metrics are different, without mentioning that the "2018" paper also obtained the 0.462 result for the smaller metric, and without mentioning that the "2018" paper was posted before the "2017" paper was.

**From:** perret <ludovic.perret@lip6.fr>
**Sent:** Tuesday, May 08, 2018 6:57 AM
**To:** pqc-comments; pqc-forum@list.nist.gov
**Subject:** Re: [pqc-forum] OFFICIAL COMMENT: GeMSS

Dear Mailing list,

We have 20 minutes to present GeMSS and DualModeMS. Contrarily to the PQC'18 presentation on:
Daniel J. Bernstein and Bo-Yin Yang: ``Asymptotically faster quantum algorithms to solve multivariate quadratic equations'', the goal of the GeMSS/DualModeMS talk was not to have an in-depth discussion about recent results on the asymptotic hardness of MQ in the quantum setting. We tried to give a global idea on the features of GeMSS & DualModeMS and explain our strategy to derive the parameters.

The purpose of the slide that is pointed by D. Bernstein was too explain the strategy for evaluating the security of GeMSS/DualModeMS in the quantum setting. In particular, we wanted to emphasize that we already used O(2^0.462m) in the reference documentation of GeMSS/DualModeMS presentation. For the record, we copy-paste below the related paragraph in the GeMMS documentation submitted to NIST (deadline was end of November 2017).
``
QuantumBooleanSolve. In a recent paper [35], the authors present a quantum version of BooleanSolve that takes advantages of Grover's quantum algorithm [44]. QuantumBooleanSolve is a Las-Vegas quantum algorithm allowing to solve a system of m boolean equations in m variables. It uses O(n) qbits, requires the evaluation of, on average, O(2^0.462m) quantum gates. This complexity is obtained under certain algebraic assumptions.
''
where [35] is:
Jean-Charles Faugère, Kelsey Horan, Delaram Kahrobaei, Marc Kaplan, Elham Kashefi, and Ludovic Perret. Fast quantum algorithm for solving multivariate quadratic equations. To appear.

We have no doubt that the PQC'18 paper was done independently. However, this paper was only available 2017.12.15; so after NIST's submission deadline.

In fact, [35] was submitted to PKC'18 and rejected with quite unfair reasons to our point of view. Anyway, the situation is as it is. [35] was only made publicly available after the PQC'18 paper.

The current version of [35] is available here: https://eprint.iacr.org/2017/1236.pdf
It is currently under revision. We will inform the list as soon as the paper is available. This will be a better basis for comments; rather than (over)interpreting the slides on GeMSS/DualModeMS; that are somewhat unrelated to the issue.

Best Regards,

Ludovic Perret, on the behalf of the authors of [35] (Jean-Charles Faugère, Kelsey Horan, Delaram Kahrobaei, Marc Kaplan, Elham Kashefi)

> Le 30 avr. 2018 à 09:44, D. J. Bernstein <djb@cr.yp.to> a écrit :
>
> I'm writing to correct some misimpressions regarding asymptotic MQ
> security that are created by the GeMSS/DualModeMS presentation: