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


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 $\log_2 3 = 0.79248...$ 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.