From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-comments@nist.gov
CC: pqc-forum@list.nist.gov
Subject: [pqc-forum] ROUND 3 OFFICIAL COMMENT: Classic McEliece
Date: Thursday, June 16, 2022 02:24:17 PM ET
Attachments: smime.p7m

The following observation may be of interest for people quantifying the stability of state-of-the-art attacks against Classic McEliece.

Our PQCrypto 2008 ISD algorithm is faster than the Eurocrypt 2022 ISD algorithm, on the CPUs selected in the new paper, for the challenges selected in the new paper, according to a direct comparison of (1) our measurements of the 2008 software (the 2+2 case of the 2008 algorithm) and (2) the speeds reported in the new paper for that paper's software.

Instructions for reproducing our measurements appear in README in the following package, along with a review of the known opportunities for further speedups: https://cr.yp.to/software/lowweight-20220616.tar.gz

The new paper's comparison to previous work does not appear to account for various speedups described in the 2008 paper, such as the usage of 2^l-bit tables and the "c" parameter. These speedups are particularly important for the 2+2 case, also influencing comparisons of the 2+2 case to other cases.

---D. J. Bernstein, T. Lange, and C. Peters

From: Andre Esser <andre.r.esser@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: D. J. Bernstein <djb@cr.yp.to>, pqc-...@list.nist.gov <pqc-forum@list.nist.gov>, pqc-co...@nist.gov <pqc-comments@nist.gov>, pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: [pqc-forum] Re: ROUND 3 OFFICIAL COMMENT: Classic McEliece
Date: Tuesday, June 21, 2022 07:17:10 AM ET

We never claimed that advanced ISD procedures in the *low-memory regime* (2+2 case) would yield significant improvements over Stern- or Dumer-like decoding.

Citation from our Eurocrypt 2022 paper:
"We find that our implementation performs 12.46 and 17.85 times faster on the McEliece-1284 challenge and 9.56 and 20.36 times faster on the McEliece-1223 instance than [other *Dumer* implementations]"

>>The following observation may be of interest for people quantifying the stability of state-of-the-
>>art attacks against Classic McEliece.

Our work already shows "stability" in the sense that even though McEliece parameters were selected according to a 60 year old algorithm, they miss the security levels only by a few bits. However, the claimed stagnation makes the assumption that the 2+2 case would be the relevant one for McEliece security estimates. Where it is the *high-memory regime* which yields the speedups. Our results show that already for code length of about 1400 the high memory regime yields improvements in practice. Hence, it cannot be neglected entirely in the security analysis.

>>Our PQCrypto 2008 ISD algorithm is faster than the Eurocrypt 2022 ISD algorithm [...]

According to the uploaded benchmarks by not even 20%. However, inspecting the code reveals that it is highly specialized and optimized for the *low-memory regime*. Opposed to our code, which allows

for high-memory instantiations.

A tuning to the special case together with the mentioned (only 2+2 relevant) improvements is likely

to bring us back to the above speedup range. Especially, since we already improved our

implementation by a factor of about 2.5. However, as said, an optimization for the high-memory

case is the way to go when focussing on McEliece security.

-Andre (speaking for myself)

D. J. Bernstein schrieb am Donnerstag, 16. Juni 2022 um 22:23:59 UTC+4:

> The following observation may be of interest for people quantifying the
> stability of state-of-the-art attacks against Classic McEliece.
>
> Our PQCrypto 2008 ISD algorithm is faster than the Eurocrypt 2022 ISD
> algorithm, on the CPUs selected in the new paper, for the challenges
> selected in the new paper, according to a direct comparison of (1) our
> measurements of the 2008 software (the 2+2 case of the 2008 algorithm)
> and (2) the speeds reported in the new paper for that paper's software.
>
> Instructions for reproducing our measurements appear in README in the
> following package, along with a review of the known opportunities for
> further speedups: https://cr.yp.to/software/lowweight-20220616.tar.gz
>
> The new paper's comparison to previous work does not appear to account
> for various speedups described in the 2008 paper, such as the usage of
> 2^l-bit tables and the "c" parameter. These speedups are particularly
> important for the 2+2 case, also influencing comparisons of the 2+2 case
> to other cases.
>
> ---D. J. Bernstein, T. Lange, and C. Peters

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/e95f5ee8-9562-47d1-a19c-c0eb12c139a4n%40list.nist.gov.