
From: Ward Beullens <ward.beullens@student.kuleuven.be>
Sent: Saturday, December 23, 2017 5:43 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: DME

Dear all,

There seems to be a mistake in the `dme_implementation` document. The irreducible polynomial $S^3 + cS^2 + dS + e$ defined at page 3 is in fact not irreducible.

The constants `c` and `d` in the document do not agree with the value in the reference implementation (which are likely the correct values because they do define an irreducible polynomial).

Kind regards,

--

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.

Visit this group at <https://groups.google.com/a/list.nist.gov/group/pqc-forum/>.