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 + c S^2 + d S + 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,