From: CLX Team <clx.lightcryptography@gmail.com>
Sent: Friday, April 19, 2019 8:05 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: CLX
Attachments: CLX-round1-correction1.pdf

Dear NIST,

Please note that there are two errors in the CLX report that may affect your reading of the report:

1) the key loading in Subsection 1.4.1 is incorrect for 192-bit or 256-bit key, which has been corrected in our reference implementations.

2) the hardware area of CLX-192Q in Table 4.1 is incorrect.

Please refer to the attached 'CLX-round1-correction1.pdf' file for the details and the correction.

Best regards,
CLX Team

Corrections to CLX Round 1 Report

Hongjun Wu and Tao Huang

19 April 2019

1 Correction to the key setup in Subsection 1.4.1 on Page 10

The original key setup is:

==========

1. Set the (160+x)-bit state S as 0.
2. Set $s_{31+x} = 1$.
3. Set $s_{\{32+x,127+2x\}} = k_{\{0,95+x\}}$.
4. Update the state using Permu3

==========

The correct key setup should be:

1. Set the (160+x)-bit state S as 0.
2. Set $s_{63} = 1$.
3. Set $s_{\{64,159+x\}} = k_{\{0,95+x\}}$.
4. Update the state using Permu3

Reason for this correction: When a 192-bit or 256-bit key is loaded into the state, part of the key is not loaded into the state.

2 Correction to the hardware area of CLX-192Q in Table 4.1 on Page 26

The original hardware area of CLX-192Q (8 rounds) in the report is given as: 1743 GE.
The hardware area of CLX-192Q (8 rounds) should be changed to: 2146 GE.