From: Alperin-Sheriff, Jacob (Fed)
Sent: Friday, February 16, 2018 10:45 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Lizard

Lizard Team:

The CDF_TABLE parameters in your specification documents don't appear to match the parameters in the code. This should be explained and clarified (on the forum I suppose since you don't appear to have an external website).

—Jacob Alperin-Sheriff

From: 김두형 <duhyeong1204@gmail.com>
Sent: Friday, February 23, 2018 3:40 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov; 이주희 연구원_서울대; Jung Hee Cheon; 윤아람 교수님; 김준섭
Subject: OFFICIAL COMMENT: Lizard
Attachments: Lizard_table_revised.pdf

Reply on the comment from Jacob Alperin-Sheriff:

Dear Jacob,

Thank you for pointing out the mistake on our tables.

The previous “CDF_table" actually described the PDF of the error distribution (for x >= 0 since it is symmetric), but we missed to explain the difference.

We corrected “CDF_table” in our supplement documentation following that in our reference/optimized code.

You can find the revised documentation in attachment.

Thanks.

Sincerely,

Duhyeong Kim
Department of Mathematical Sciences
Seoul National Uni
versity (Bdg 27, Rm 441)
Phone: +82-2-880-6272
E-mail: doodoo1204@snu.ac.kr

From: 김두형 <duhyeong1204@gmail.com>
Sent: Tuesday, February 27, 2018 11:39 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov; Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); 이주희 연구원_서울대; 천정희 교수님; 윤아람 교수님; 김준섭
Subject: OFFICIAL COMMENT: Lizard

Reply on Jacob's Comment:

Thank you for pointing out the mistake on our tables.

The "CDF_TABLE" values we gave for each instantiation of our schemes Section 4.2.3 ("Recommended Parameters") of our Supporting Documentation actually described the PDF of the error distribution (for x >= 0 since it is symmetric), rather than the CDF values that are actually used in our submitted code.

Specifically, the followings are the correct values for the CDF Tables:

Lizard.CCA

CCA_CATEGORY1_N536
CDF_LENGTH = 9
CDF_TABLE= { 78, 226, 334, 425, 473, 495, 506, 510, 511 }
CCA_CATEGORY1_N663
CDF_LENGTH = 4
CDF_TABLE = { 458, 946, 1020, 1023 }
CCA_CATEGORY1_N816
CDF_LENGTH = 5
CDF_TABLE = { 151, 382, 482, 507, 511 }
CCA_CATEGORY1_N952
CDF_LENGTH = 6
CDF_TABLE = { 121, 325, 445, 494, 508, 511 }
CCA_CATEGORY1_N1088
CDF_LENGTH = 12
CDF_TABLE = { 262, 761, 1188, 1518, 1748, 1892, 1974, 2016, 2035, 2043, 2046, 2047 }
CCA_CATEGORY1_N1300
CDF_LENGTH = 4
CDF_TABLE = { 380, 874, 1008, 1023 }

Lizard.KEM

KEM_CATEGORY1_N536
CDF_LENGTH = 9
CDF_TABLE= { 78, 226, 334, 425, 473, 495, 506, 510, 511 }
KEM_CATEGORY1_N663
CDF_LENGTH = 4
CDF_TABLE = { 458, 946, 1020, 1023 }
KEM_CATEGORY1_N816
CDF_LENGTH = 5
CDF_TABLE = { 151, 382, 482, 507, 511 }
KEM_CATEGORY1_N952
CDF_LENGTH = 6

CDF_TABLE = { 121, 325, 445, 494, 508, 511 }
KEM_CATEGORY1_N1088
CDF_LENGTH = 12
CDF_TABLE = { 262, 761, 1188, 1518, 1748, 1892, 1974, 2016, 2035, 2043, 2046, 2047 }
KEM_CATEGORY1_N1300
CDF_LENGTH = 4
CDF_TABLE = { 380, 874, 1008, 1023 }

RLizard.CCA and RLizard.KEM
RING_CATEGORY1
CDF_LENGTH = 4
CDF_TABLE= { 190, 437, 504, 511 }
RING_CATEGORY3_N1024
CDF_LENGTH = 6
CDF_TABLE = { 279, 722, 941, 1009, 1022, 1023 }
RING_CATEGORY3_N2048
CDF_LENGTH = 8
CDF_TABLE = { 407, 1127, 1623, 1889, 2000, 2036, 2045, 2047 }
RING_CATEGORY5
CDF_LENGTH = 10
CDF_TABLE = { 154, 443, 676, 838, 936, 987, 1010, 1019, 1022, 1023 }

Best,

Duhyeong Kim
Department of Mathematical Sciences
Seoul National University (Bdg 27, Rm 441)
Phone: +82-2-880-6272
E-mail: doodoo1204@snu.ac.kr