From: Minhye Seo <smh89122@hanmail.net>
Sent: Thursday, April 12, 2018 7:44 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: EMBLEM and R.EMBLEM

Dear all,

According to the recent result of SafeCrypto website, we have changed the parameters for our submission in order to provide at least 128-bit security level.

Here's the modified parameter sets for EMBLEM and REMBLEM.

	EMBLEM	**EMBLEM**	**EMBLEM**	**EMBLEM**	**R.EMBLEM**	**R.EMBLEM**
Secret distribution	[-1,1]	[-1,1]	[-2,2]	[-2,2]	[-1,1]	[-1,1]
m	1186	1008	1210	1016	-	-
n	1024	824	984	784	512	1024
log(q)	24	20	24	20	16	14
Sigma	25	25	25	25	29	3
t	8	4	8	4	1	1
|PK| size	28,496	20,192	29,072	20,352	1,056	1,824
|SK| size	32	32	32	32	32	32
|CT| size	12,416	16,672	11,936	15,872	1,568	2,272

Sincerely,
The EMBLEM team