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

From: D. J. Bernstein <djb@cr.yp.to>
Sent: Thursday, November 22, 2018 3:57 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: EMBLEM and R.EMBLEM
Attachments: signature.asc

Table 6 of the R.EMBLEM specification specifies two parameter sets with n=512. The table says that these have

* 1056-byte and 928-byte public keys respectively,
* 32-byte secret keys in both cases, and
* 1568-byte and 1376-byte ciphertexts respectively.

Each of the R.EMBLEM implementations in the submission appears to use
n=512 with the first or second parameter set from the table (varying between reference and optimized implementations), but with

* much larger public keys,
* much larger secret keys, and
* much larger ciphertexts.

These three gaps appear to be explained by the following three major discrepancies between the specification and the implementations:

* The specification (footnote on page 8) says that the secret key "can be generated" from a short seed. The claimed secret-key size suggests that this uses a 32-byte seed.

  However, this seed expansion isn't specified in detail and isn't implemented. The implementation uses a much longer secret key that encodes not just cipher output but also the results of some precomputation.

* The specification (same footnote) also says that one of the components of the public key "can also be derived from the seed by using PRF".

  This description is inadequate. There have to be two layers, first producing a public seed from the secret seed, second expanding the public seed into this component of the public key.

  The claimed public-key size suggests that the public seed is also 32 bytes. However, the expansion isn't specified in detail and isn't implemented.

* The claimed public-key size and ciphertext size suggest that integers mod q are encoded as 14 bits for q=12289 or 16 bits for q=40961.

  However, the encoding details aren't specified. What's implemented is 32 bits.

The space claimed in the specification clearly involves various extra computations, especially for decapsulation. Proper benchmarking needs to include the cost of these computations. Also, the details can create security problems, so it's important for security evaluation to have the details fully specified and implemented.

To have something to benchmark that isn't _obviously_ out of whack with the specification, I've made various changes to the R.EMBLEM code to

 * store a 32-byte secret key, which is then expanded into the
 previous key;
 * store the first component of the public key as a 32-byte seed,
 which is then expanded; and
 * use a packed 14-bit/16-bit encoding for public key and ciphertext,

producing "remblem928" and "remblem1056" in the next version of SUPERCOP.
Of course it's possible that I've accidentally introduced security problems and/or deviations from the things that _were_ specified.

Four further R.EMBLEM parameter sets with smaller values of n, such as n=504, are listed in Table 5 of the specification. When n is not a power of 2, the specification is wrong in describing x^n+1 as a cyclotomic polynomial, and the specification fails to analyze known attack techniques that exploit the factorization of x^n+1.

Two additional R.EMBLEM parameter sets appear in new software on the EMBLEM/R.EMBLEM web page. As noted earlier, NIST has stated that "the selection of candidates for the second round will primarily be based on the original submissions", so I've focused on the original parameters.
The software on the web page doesn't seem to resolve any of the issues regarding secret expansion, public expansion, and integer encodings.

I presume that many of the R.EMBLEM issues described above also apply to EMBLEM, but I haven't looked at the EMBLEM details.

---Dan

--
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/.