FrodoKEM

(Round 2)

Carl A. Miller
NIST Computer Security Division

May 21, 2019

NIST PQC Seminar (not for public distribution)

Learning With Errors (LWE) encryption

CRYSTALS-KYBER
FrodoKEM
LAC
NewHope
NTRU
NTRU Prime
Round5
SABER
Three Bears

The Protocol

Basic LWE assumption: Suppose that A is a random m x n matrix, S is a random n x p matrix, and

$$B = AS + E,$$

where E is Gaussian. Then, given A, the matrix B is indistinguishable from random.

The Protocol

Basic LWE assumption: Suppose that A is a random m x n matrix, S is a ~~random~~ n x p matrix, and

Gaussian

$$B = AS + E,$$

where E is Gaussian. Then, given A, the matrix B is indistinguishable from random.

This is "normal form" LWE.

The Protocol

Suppose that Bob has a message μ.
He encodes it into the **most significant bits** of the entries of a matrix M.
He generates two new LWE samples (one from A, one from B) and adds M to the 2nd one.

A, B, S

S'A + E'
S'B + E'' + M

A and B (:= AS + E),

The Protocol

Alice can now decode (provided that the errors introduced by the Gaussian matrices didn't confuse the message).

A, B, S

S'A + E'

S'B + E'' + M

A and B (:= AS + E),

The Protocol

This is IND-CPA encryption.

Via the Fujisaki-Okamoto transform + hash functions, the authors then give a KEM protocol that they claim to be IND-CCA2.

Subroutines

The matrix A is actually generated from a pseudorandom seed (via AES or SHAKE). The seed is part of the public key.

The hashing used in the Fujisaki-Okamoto transform is done with SHAKE.

What's different about FrodoKEM?

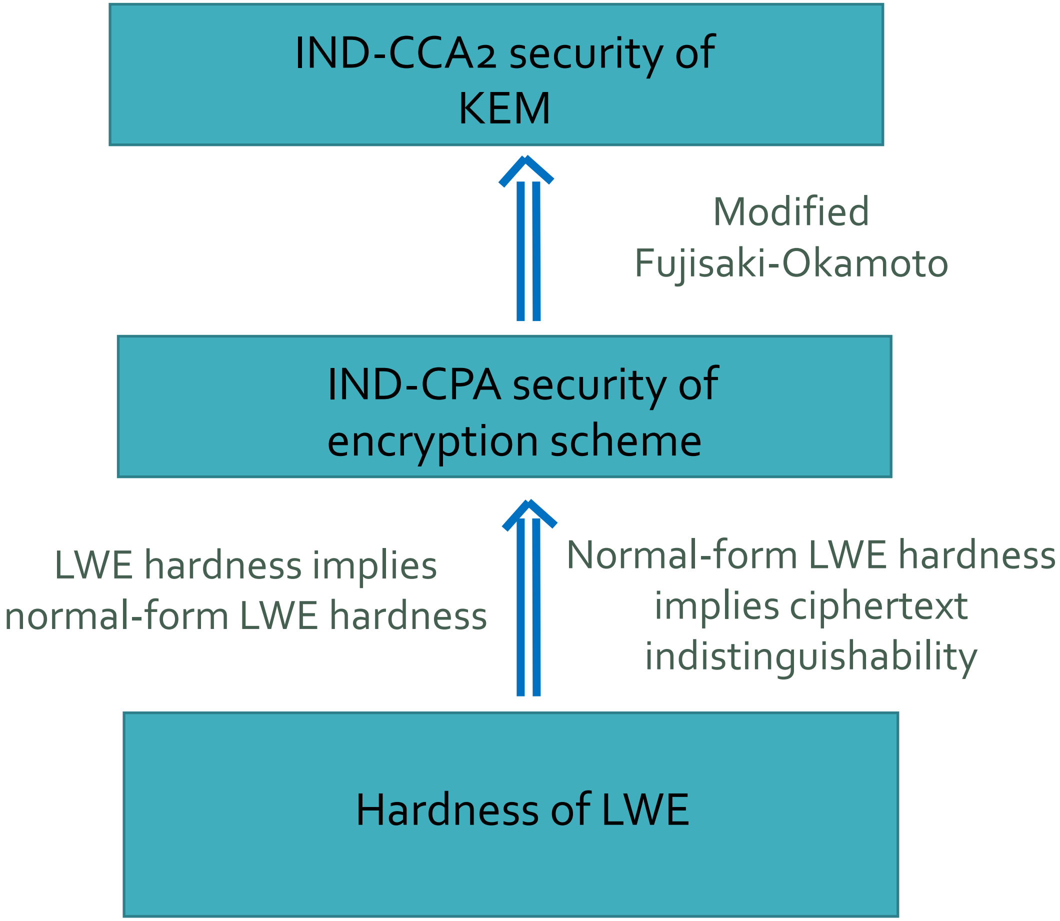
- It uses an unstructured version of LWE (as opposed to module or ring LWE).

- The encoding mechanism?

- Anything else?

The main change from Round 1 appears to be the introduction of Level 5 security.

Security Analysis



The second layer requires the quantum random oracle model for the hash functions.

Comments

From: D. J. Bernstein <djb@cr.yp.to>
Sent: Saturday, April 21, 2018 6:16 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Frodo
Attachments: signature.asc

Summary: The "FrodoKEM" submission claims that various theorems support the security of the submission. This claim is incorrect for at least two of the stated theorems: these two theorems do not, in fact, support the security of the submission.

The exact quote at issue is in Section 5.1:

> 5 Justification of security strength
>
> The security of FrodoKEM is supported both by security reductions and by analysis of the best known cryptanalytic attacks.
>
> 5.1 Security reductions
>
> A summary of the reductions supporting the security of FrodoKEM is as follows: ... Theorem 5.2 gives a non-tight, classical reduction against quantum adversaries in the quantum random oracle model. ... Theorem 5.8 gives a non-tight classical reduction against classical or quantum adversaries (in the standard model).

Comments

From: cpeikert@gmail.com on behalf of Christopher J Peikert <cpeikert@alum.mit.edu>
Sent: Wednesday, April 25, 2018 2:48 PM
To: pqc-forum; pqc-comments
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Frodo

The FrodoKEM submission distinguishes between:

1. the freely parametrizable FrodoPKE/KEM constructions (Section 2.2), whose asymptotic security is indeed supported by a collection of tight and non-tight reductions (Section 5.1), and

2. the concrete instantiations FrodoKEM-640 and -976 (Section 2.4), whose concrete security is estimated by cryptanalysis, e.g., using the "core-SVP" methodology (Section 5.2).

(Please note that in Section 6.2 ("Compatibility with existing deployments"), the references to FrodoKEM can only make sense as referring to the concrete instantiations, but this should have been completely explicit to avoid any possibility of confusion. We believe there aren't any such ambiguities in the rest of the submission.)

Our approach, of starting from a parametrizable construction with asymptotic security supported by (possibly loose) reductions and then instantiating its parameters via cryptanalysis, is motivated and explained in detail in Section 1.2.2. Moreover, we explicitly disclaim any use of loose reductions as supporting the concrete security of our instantiations. For example, Section 1.2.2 says,

> "We stress that we use the worst-case reduction only for guidance in
> choosing a narrow enough error distribution for practice that still
> has some theoretical support, and not for any concrete security claim.
> ... Instead, as stated in the above quote from [85], we choose
> concrete parameters using a conservative analysis of the best known
> cryptanalytic attacks, as described next."

Therefore, we believe there should not be any confusion about what the submission does and does not claim (and even disclaims) as justification for the concrete security of the FrodoKEM instantiations.

Performance

Speed (in thousands of cycles):

	Scheme	KeyGen	Encaps	Decaps	Total (Encaps + Decaps)
	Optimized Implementation (AES from OpenSSL)				
Security level 1	FrodoKEM-640-AES	1,384	1,858	1,749	3,607
Security level 3	FrodoKEM-976-AES	2,820	3,559	3,400	6,959
Security level 5	FrodoKEM-1344-AES	4,756	5,981	5,748	11,729

This is the AES version. (The SHAKE version is considerably slower.)

Performance

Memory usage (in bytes):

Scheme	Peak stack memory usage KeyGen	Peak stack memory usage Encaps	Peak stack memory usage Decaps	Static library size
Optimized Implementation (AES from OpenSSL)				
FrodoKEM-640-AES	72,448	102,944	123,968	68,668
FrodoKEM-976-AES	111,424	158,944	189,080	66,236
FrodoKEM-1344-AES	152,688	216,552	259,784	64,732

Performance

Message & key sizes (in bytes):

Scheme	**secret key** sk	**public key** pk	**ciphertext** c	**shared secret** **ss**
FrodoKEM-640	19,888 (10,256 + 9,616 + 16)	9,616 (16 + 9,600)	9,720 (9,600 + 120)	16
FrodoKEM-976	31,296 (15,640 + 15,632 + 24)	15,632 (16 + 15,616)	15,744 (15,616 + 128)	24
FrodoKEM-1344	43,088 (21,536 + 21,520 + 32)	21,520 (16 + 21,504)	21,632 (21,504 + 128)	32

Performance

Decryption failure probability:

	failure prob.
Frodo-640	$2^{-138.7}$
Frodo-976	$2^{-199.6}$
Frodo-1344	$2^{-252.5}$

The authors claim that the problem of information-leakage via intentional decryption failures has been explored, and is not a threat (subsection 5.2.4).

FrodoKEM

(Round 2)

Carl A. Miller
NIST Computer Security Division

May 21, 2019

NIST PQC Seminar (not for public distribution)