National Institute of Information and Communications Technology, Japan

LOTUS: an LWE-based PKE/KEM

Submitters

Le Trieu Phong, Takuya Hayashi,

Yoshinori Aono, Shiho Moriai

LOTUS

Learning with errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era

- PKE and KEM
- IND-CCA2 security, based on the LWE assumption.
- Parameter sets for 128-bit, 192-bit, 256-bit securities.
- Can even set parameters for >256-bit security.

- **The distinction of LOTUS**: among encryption schemes based on the LWE assumption (Regev 2005), LOTUS has the **smallest ciphertexts** (1.1∼1.7 KB + size(symmetric part)).

At the heart of LOTUS

- In our paper at INDOCRYPT 2013, we present the idea of combining:

  Lindner-Peikert 2011 + Fujisaki-Okamoto 2013

  For using the LWE For CCA security

- LOTUS is the continuation of the idea, in which new parameter sets are introduced, to obtain:
  - Decryption error < 2^{-256}.
  - 128-, 192-, 256-bit securities (hardness) of the LWE assumption.

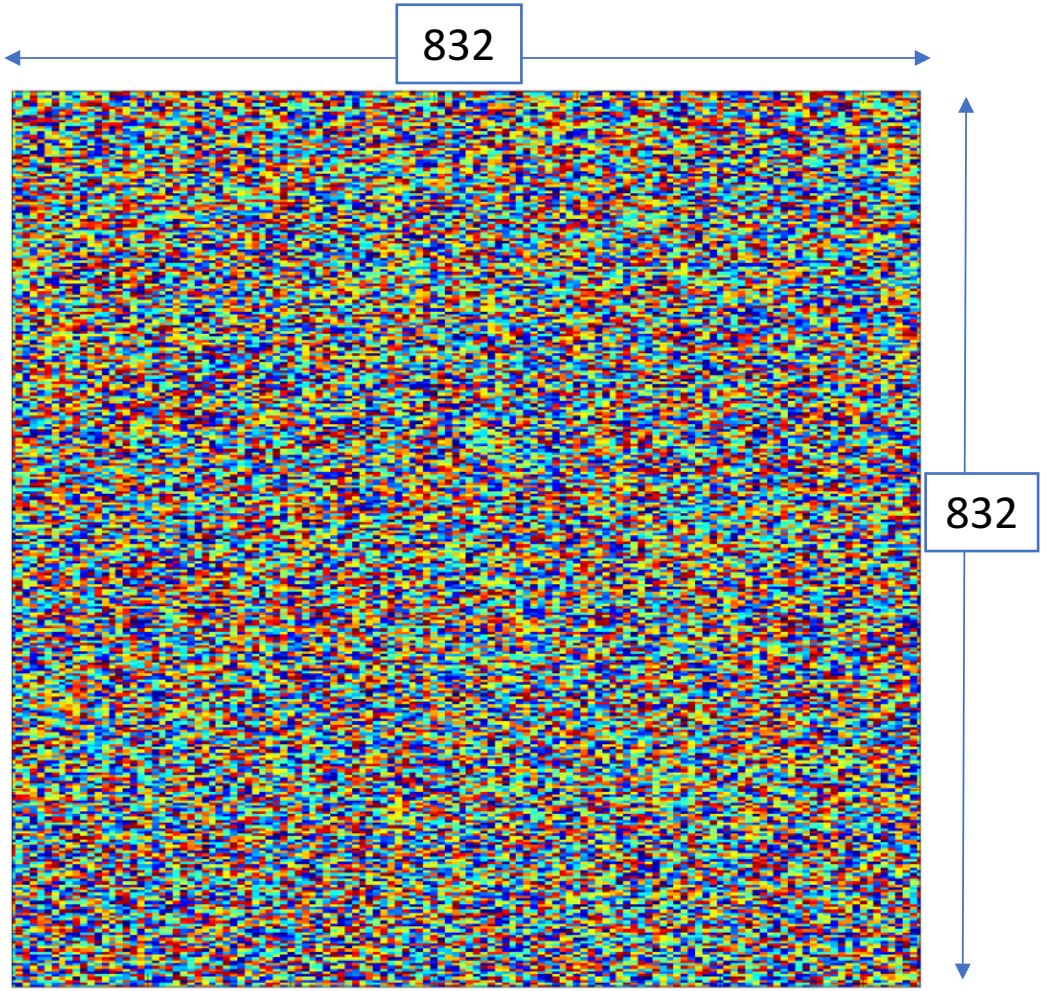
Y. Aono, X. Boyen, L. T. Phong, L. Wang: Key-Private Proxy Re-encryption under LWE. INDOCRYPT 2013
R. Lindner, C. Peikert: Better Key Sizes (and Attacks) for LWE-Based Encryption. CT-RSA 2011
E. Fujisaki, T. Okamoto: Secure Integration of Asymmetric and Symmetric Encryption Schemes. J. Cryptology (2013)

Notations

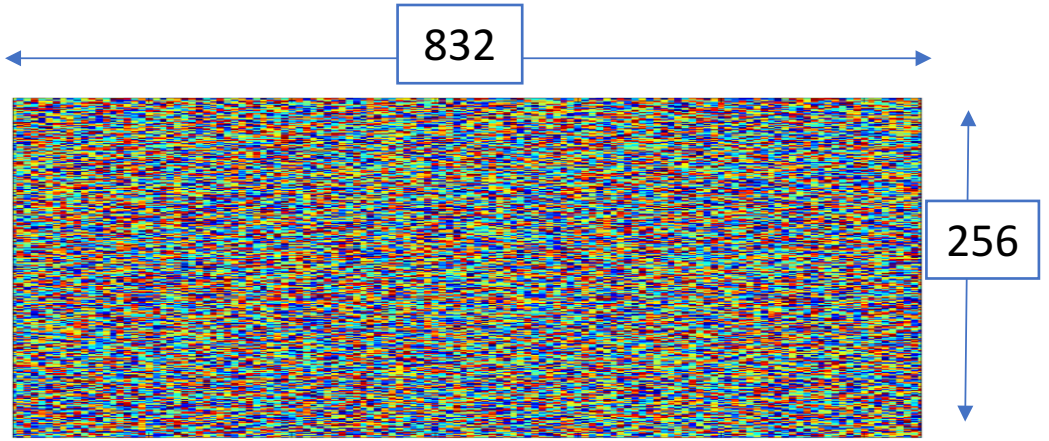
n, q, s	LWE parameters
l	An integer in {128, 192, 256}
A	A random matrix in $Z_q^{n \times n}$
P	A matrix in $Z_q^{n \times l}$

LOTUS key generation of (A, P, n, q, l, s)

$A =$



$$P = R - AS \in Z_q^{n \times l}$$



- $n = 832$: LWE
- $q = 8192$: modulus
- $l = 256$: AES key length
- $s = 3$: Gaussian noise

LOTUS encryption of $m \in \{0,1\}^*$

$$\mathsf{Enc}^{cca}_{pk}(m;\sigma) = \Big(\underbrace{\mathsf{Enc}^{cpa}_{pk}\Big(\sigma; H(\sigma \parallel c_{sym})\Big)}_{(c_1,c_2)}, \underbrace{\mathsf{SE}_{G(\sigma)}(m)}_{c_{sym}} \Big)$$

LOTUS encryption of arbitrary message m with randomness σ

Lindner-Peikert2011 encryption of σ with randomness $H(\sigma \parallel c_{sym})$

AES-CTR with key $G(\sigma)$

$$c_1 = e_1 A + e_2 \in Z_q^n$$
$$c_2 = e_1 P + e_3 + \sigma \cdot \left\lfloor \frac{q}{2} \right\rfloor \in Z_q^l$$

Lindner-Peikert2011 + Fujisaki-Okamoto2013

LOTUS decryption of (c_1, c_2, c_{sym})

- Compute $\bar{\sigma} = c_1 S + c_2 \in Z_q^l$
- Compute $\sigma' \in \{0,1\}^l$
- Integrity check

$$(c_1, c_2) = Enc_{pke}^{cpa}(\sigma'; H(\sigma' \parallel c_{sym}))$$

1. Return fail if the check does not pass
2. Return $m = SD_{G(\sigma)}(c_{sym})$ if the check does pass

Parameters

	LWE's (n, q, s)	Others	NIST's category
`lotus-params128`	$(n = 576, q = 8192, s = 3)$	$l = KeyLen = 128$	AES-128, SHA3-256
`lotus-params192`	$(n = 704, q = 8192, s = 3)$	$l = KeyLen = 192$	AES-192, SHA3-384
`lotus-params256`	$(n = 832, q = 8192, s = 3)$	$l = KeyLen = 256$	AES-256

Claim 1 (statistically negligible decryption error):

The decryption error due to large noise in LOTUS is less than 2^{-256} for all `lotus-params{128,192,256}`.

Note:

With $q = 8192$ and $s = 3$, the same claim holds for all $n \leq 1800$. Therefore, there is a lot of space to increase the LWE security parameter n.

Parameters

	LWE's (n, q, s)	Others	NIST's category
`lotus-params128`	$(n = 576, q = 8192, s = 3)$	$l = KeyLen = 128$	AES-128, SHA3-256
`lotus-params192`	$(n = 704, q = 8192, s = 3)$	$l = KeyLen = 192$	AES-192, SHA3-384
`lotus-params256`	$(n = 832, q = 8192, s = 3)$	$l = KeyLen = 256$	AES-256

Claim 2 (IND-CCA2 security):

LOTUS achieves IND-CCA2 security under the LWE(n, q, s) assumption in the random oracle model.

Note:

This is thanks to the IND-CPA security of Lindner-Peikert2011 and the transformation in Fujisaki-Okamoto2013.

Parameters

	LWE's (n, q, s)	Others	NIST's category
`lotus-params128`	$(n = 576, q = 8192, s = 3)$	$l = KeyLen = 128$	AES-128, SHA3-256
`lotus-params192`	$(n = 704, q = 8192, s = 3)$	$l = KeyLen = 192$	AES-192, SHA3-384
`lotus-params256`	$(n = 832, q = 8192, s = 3)$	$l = KeyLen = 256$	AES-256

Claim 3 (LWE practical hardness):

We estimate the LWE(n, q, s) assumption with parameters in the above table satisfy the corresponding NIST's security categories.

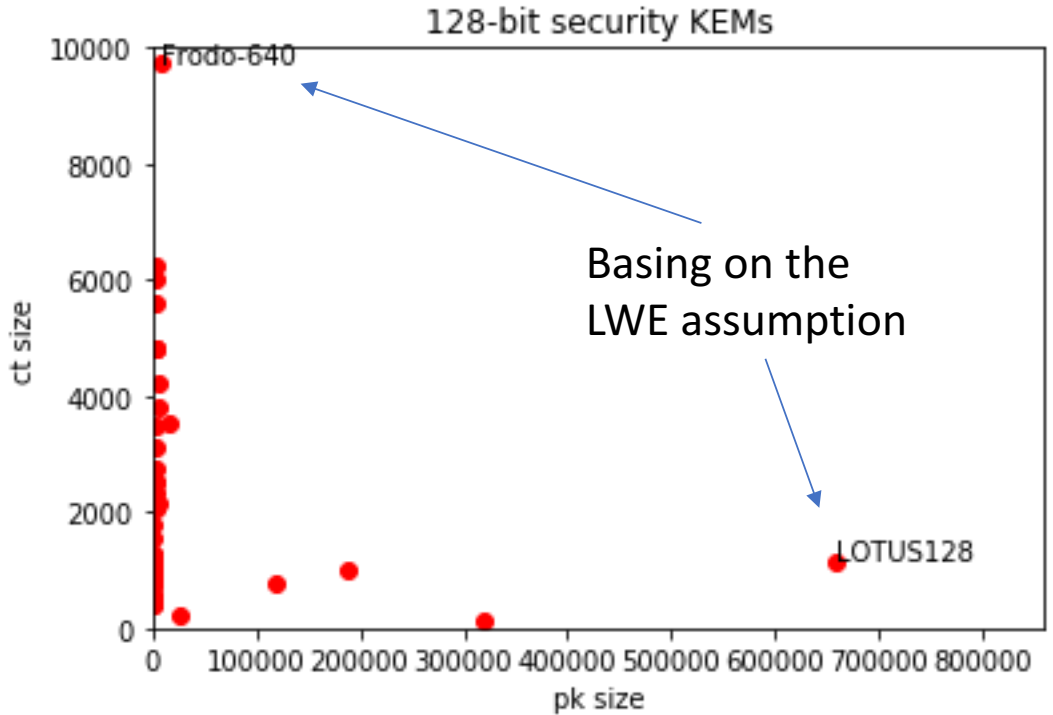
Note:

This is thanks to a long line of research on estimating the practical hardness of LWE, including ours.

LOTUS-PKE sizes and a comparison

Table 4. LOTUS-PKE sizes.

Parameter set	Public key size	Secret key size	Encapsulation size
`lotus-params128`	658.95 (KB)	700.42 (KB)	1.144 (KB) + $size(c_{sym})$
`lotus-params192`	1025.0 (KB)	1101.0 (KB)	1.456 (KB) + $size(c_{sym})$
`lotus-params256`	1471.0 (KB)	1590.8 (KB)	1.768 (KB) + $size(c_{sym})$



LOTUS speed (already fast enough)

Parameter set	$\mathsf{KeyGen}_{pke}^{cca}$	Enc_{pke}^{cca}	Dec_{pke}^{cca}
`lotus-params128`	6,385.842 usec 26,820,400 clock	75.299 usec 316,252 clock	91.091 usec 382,582 clock
`lotus-params192`	11,109.302 usec 46,658,849 clock	105.636 usec 443,667 clock	139.862 usec 587,417 clock
`lotus-params256`	17,197.583 usec 72,229,496 clock	149.075 usec 626,112 clock	210.126 usec 882,523 clock

(usec denotes microsecond.)

LOTUS

Learning with errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era

- PKE and KEM
- IND-CCA2 security, based on the LWE assumption.
- Parameter sets for 128-bit, 192-bit, 256-bit securities.
- Can even set parameters for >256-bit security.

- **The distinction of LOTUS**: among encryption schemes based on the LWE assumption (Regev 2005), LOTUS has the **smallest ciphertexts** (1.1∼1.7 KB + size(symmetric part)).