SCIS 2018 2018 Symposium on
Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics,
Information and Communication Engineers

Performance Evaluation of liboqs in Open Quantum Safe Project (Part I)

Hyeongcheol An [*] Rakyong Choi [†] Jeeun Lee [†] Kwangjo Kim [*†]

Abstract: Famous public key cryptosystem such as RSA and Diffie-Hellman is not secure against quantum computer. Also, the emergence of quantum computers is not theoretical but is actually in practical. Post-Quantum Cryptography (PQC) means quantum-resistant cryptography. Lattice-based cryptography has been known as one of PQC. Learning with Errors (LWE), Ring Learning with Errors (Ring-LWE), and Module Learning with Errors(Module-LWE) are the mathematical hard problems in lattice-based cryptography. In public domain, Open Quantum Safe (OQS) project develops quantum-resistant cryptosystems such as lattice-based, code-based, and supersingular isogeny elliptic curve as open source. We focus on lattice-based OQS projects such as BCNS15, NewHope, MSrln, Kyber, and Frodo. In this paper, we check and compare the performance of OQS key exchange protocols using lattices. Then, we suggest future work in OQS project.

Keywords: Open Quantum Safe project, lattice-based, code-based, SIDH, key exchange protocol

1 Introduction

1.1 Motivation

IBM has developed a quantum computer that allows the public to simulate a quantum computer through an IBM cloud service. IBM developed a quantum computer with 5-qubit in 2016 and a new quantum computer with 50-qubit in Nov., 2017. Therefore, the emergence of quantum computers is not theoretical but becomes actually in practical.

Public key cryptosystems such as RSA and Diffie-Hellman (DH) key exchange protocol are based on the difficulty of Integer Factorization Problem (IFP) and Discrete Logarithm Problem (DLP). However, IFP and DLP can be solved within the polynomial time by Shor's algorithm[1] using a quantum computer. Blockcipher such as AES and DES can be solved using Grover's algorithm.[2]. Grover's algorithm can use data search problem. In classical computer, adversary can search database as $O(2^n)$ complexity. Using the quantum computer, the complexity of data search problem reduces just $O(\sqrt{2^n})$. Therefore, current cryptosystems must be replace due to defense the quantum adversary. We prepare the new cryptosystem called Post Quantum Cryptography (PQC). PQC has 5 kinds of primitives such as lattice-based, code-based, hash-based, multivariate-based, and supersingular isogeny elliptic curve. Lattice-based cryptography is used for an encryption scheme, signature, and key exchange protocol.

The National Institute of Standards and Technology (NIST) contested a public PQC cryptographic algorithm project until November 30, 2017 to select secure cryptographic algorithm against the quantum adversary. The cryptographic algorithms must provide at least one of the public key encryption, key exchange protocol, or signature. In addition, the algorithm must be secure both in the classical and quantum computing, and security level of the algorithm is at least 256-bit.

We investigate the cryptographic features of 9 kinds of key exchange protocols such as Frodo[3], BCNS[4], NewHope[5], MSrln[6], Kyber[7], NTRU[8] McBits[9], IQC[10], and MSR SIDH[11] in Open Quantum Safe (OQS) project. OQS project is based on three kinds of PQC primitives such as lattice-based, code-based, and supersingular isogeny elliptic curve. Frodo, BCNS, NewHope, MSrln, Kyber, and NTRU key exchange protocol are based on lattice-based scheme. IQC and MSR SIDH are based on supersingular isogeny elliptic curve scheme. McBits is based on code-based scheme. In this paper, we introduce contents of OQS project. Then, we experiment with each protocol as payload and runtime.

1.2 Outline of the Paper

In Section 2, we introduce lattice-based cryptography such as well-known mathematical hard problems like Learning with Errors (LWE), Ring-LWE, and Module-LWE problems. Section 3 describes related work such as PQC cryptosystems and OpenSSL library. Then, we investigate Open Quantum Safe project from the view of content and performance which contains quantum-resistant key exchange protocol in Section 4. We suggest future work and conclusion in Section 5.

[*] Graduate School of Information Security, KAIST. 291, Daehak-ro, Yuseong-gu, Daejeon, South Korea 34141. $\{anh1026, kkj\}$@kaist.ac.kr)

[†] School of Computing, KAIST. 291, Daehak-ro, Yuseong-gu, Daejeon, South Korea 34141. $\{thepride, jeeun.lee, kkj\}$@kaist.ac.kr

2 Background

In this section, the well-known lattice-based mathematical hard problem such as LWE, Ring-LWE, and Module-LWE problems will be described in brief.

Lattice-based cryptography is one of the most popular PQC primitives. Therefore, lattice-based cryptography is secure against the quantum adversary. There are many kinds of lattice-based cryptographic primitives such as Learning with Errors (LWE), Ring Learning with Errors (Ring-LWE), Module Learning with Errors (Module-LWE), Learning with Rounding (LWR), and so on. Lattice-based cryptography can be used not only for encryption scheme but also for key exchange protocol and digital signature. We will describe LWE, Ring-LWE, and Module-LWE problems in brief.

2.1 Learning with Errors

LWE problem is introduced by Regev[12] in 2009. LWE is a quantum-resistant mathematical hard problem against the quantum adversary.

Error distribution χ over $\mathbb{Z}$ is usually used Gaussian distribution or binomial distribution. LWE distribution $A_{\mathbf{s},\chi} \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n$, for a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ and choose uniformly random $\mathbf{a} \in \mathbb{Z}_q^n$, and choosing $e \leftarrow \chi$. and outputting;

$$(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \mod q)$$

LWE problem has two kinds of version such as search and decision. In cryptography, we use decision version LWE problem. Decision LWE problem is given m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n$. $A_{s,\chi}$ for a uniformly random $s \in \mathbb{Z}_q^n$ or uniform distribution, distinguish which chooses the sample.

2.2 Ring Learning with Errors

Ring-LWE problem is introduced by Lyubashevsky *et al.*[13] in 2010. Ring-LWE is also a quantum-resistant mathematical hard problem against the quantum adversary.

For a ring $\mathcal{R}$ of degree n over $\mathbb{Z}$, and defining quotient ring $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Error distribution χ over $\mathbb{Z}$ is usually used Gaussian distribution or binomial distribution. Ring-LWE distribution $A_{s,\chi} \in \mathcal{R}_q \times \mathcal{R}_q$, secret vector $s \in \mathcal{R}_q$ and choose uniformly random $a \in \mathcal{R}_q$, and choosing $e \leftarrow \chi$. and outputting;

$$(a, b = s \cdot a + e \mod q)$$

Ring-LWE problem has two kinds of version such as search and decision. In cryptography, we use decision version Ring-LWE problem. Decision Ring-LWE problem is given m independent samples $(a_i, b_i) \in \mathcal{R}_q \times \mathcal{R}_q$. $s \in A_{s,\chi}$ for a uniformly random $\mathcal{R}_q$ or uniform distribution, distinguish which chooses the sample.

2.3 Module Learning with Errors

Module-LWE problem is introduced by Langlois *et al.*[14] in 2015. Module-LWE is also a quantum-resistant mathematical hard problem against the quantum adversary.

For a ring $\mathcal{R}$ of degree n over $\mathbb{Z}$, and defining quotient ring $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Error distribution χ over $\mathbb{Z}$ is usually used Gaussian distribution or binomial distribution. Module-LWE distribution $A_{m,k,\eta} \in \mathcal{R}_q^{m\times k} \times \mathcal{R}_q^m$, secret vector $s \in \beta_\eta^k$ and choose uniformly random $a_i \in \mathcal{R}_q^k$, and choosing $e_i \leftarrow \beta_\eta$. and outputting;

$$(a, b_i = a_i^T \cdot s + e_i \mod q)$$

Module-LWE problem has two kinds of version such as search and decision. In cryptography, we use decision version Module-LWE problem. Decision Module-LWE problem is given m independent samples $(a_i, b_i) \in \mathcal{R}_q^k \times \mathcal{R}_q$. $s \in \beta_\eta^k$ for a uniformly random $\mathcal{R}_q$ or uniform distribution, distinguish which chooses the sample.

3 Related Work

3.1 OpenSSL

OpenSSL is a software library for secure communication such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocol. This library is written in C-language as open source implementation. OpenSSL supports both public key and secret key cryptography such as RSA, AES, DSA, and Elliptic Curve Diffie-Hellman (ECDH). In the current version of OpenSSL v1.1.1, DH and ECDH are implemented as key exchange protocol.

3.2 Lattice-based Key Exchange Protocol

Ding *et al.*[15] suggested the first lattice-based key exchange protocol in 2012. After this research, many works studied unauthenticated and authenticated key exchange protocols based on LWE, Ring-LWE, and Module-LWE problems.

Peikert[16] also gave efficient and practical lattice-based key exchange protocols. This protocol can be used for TLS/SSL protocol in internet.

Zhang *et al.*[17] designed a lattice-based authenticated key exchange similar to HMQV [18].

On the other hand, the first Password-based Authenticated Key Exchange (PAKE) protocol was first suggested by Bellovin and Merritt [19] without formal security analysis. PAKE protocol is advantage for its simple use. However, it has disadvantage the called dictionary attacks. In dictionary attacks, the adversary tries all possible combination of secret keys in a small set of values like a dictionary, to break the PAKE protocol. Dictionary attack is not effective in high-entropy keys. However, adversary can recover the secret key using low-entropy keys.

Dictionary attacks are classified into two types: on-line and off-line dictionary attacks. To classify this problem, several protocols are designed to be secure even when the secret key is a password. The goal of PAKE protocols is to restrict the adversaries success to on-line guessing attacks and prevent off-line dictionary attacks. The security of these protocol managements relies on policies that invalidate or block password usage if a certain number of failed attempts occur.

On the other hand, there are only a small number of lattice-based PAKE protocols. One of these lattice-based PAKE protocols is that of Katz *et al.*[20]. This protocol is proven secure in the standard model security, but it is not efficient due to its Common Reference String (CRS)-based design. Zhang *et al.*[21] suggested a new CRS-based PAKE protocol in 2017. This protocol use public key encryption with associated approximate smooth projective hashing.

But CRS-based protocols use complicated cryptographic tools to achieve standard model security while Random Oracle Model (ROM)-based protocols have very simple and elegant designs. Compared to those CRS-based protocols [20, 21], Ding *et al.*'s PAKE protocol [22] is more efficient since it is proven secure based on ROM.

Recently, Xu *et al.* [23] proposed the first lattice-based 3PAKE protocol extending by work of Ding *et al.* [22].

4 Open Quantum Safe Project

4.1 Contents of OQS

OQS project[24] is an open source and a consist of 9 PQC cryptography. OQS project is based on 3 kinds of PQC primitives such as lattice-based, code-based, and supersingular isogeny elliptic curve. Frodo, BCNS, NewHope, MSrln, Kyber, NTRU key exchange protocol are based on lattice-based scheme. IQC and MSR SIDH are based on supersingular isogeny elliptic curve scheme. McBits is based on code-based scheme. Table 1 describes algorithms of liboqs. To merge OpenSSL, they implement same header file form in OpenSSL.

Table 1: Algorithms of liboqs

Primitive		Protocol
Lattice-based	LWE	Frodo
	Ring-LWE	BCNS NewHope MSrln
	Module-LWE	Kyber
	NTRU	
Supersingular Elliptic Curve	SIDH	IQC Reference MSR SIDH
Code-based	Error-correcting codes	McBits

Sections from 4.1.1 to 4.1.5, we will describe lattice-based key exchange protocol in detail.

4.1.1 NewHope

Alkim *et al.*[5] proposed Ring-LWE key exchange protocol called NewHope in 2016.

Protocol 3 describes key exchange protocol of NewHope. To compute NewHope, we define $\mathsf{HelpRec}()$ and $\mathsf{Rec}()$ functions.

Let $\mathsf{CVP}_{\tilde{D}_4}(\mathbf{x} \in \mathbb{R}^4)$ is that an integer vector $\mathbf{z}$ such that is a closest vector to $\mathbf{x} : \mathbf{x} - \mathbf{Bz} \in \mathcal{V}$. The $\mathsf{HelpRec}(\mathbf{x}; b)$ is defined as follows:

$$\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{CVP}_{\tilde{D}_4}\Big(\frac{2^r}{q}(\mathbf{x} + b\mathbf{g})\Big) \mod 2^r$$

where $b \in \{0, 1\}$ is uniformly chosen random bit.

The $\mathsf{Decode}(\mathbf{x} \in \mathbb{R}^4/\mathbb{Z}^4)$ is that a bit k such that $k\mathbf{g}$ is a closest vector to $\mathbf{x} + \mathbb{Z}^4 : \mathbf{x} - k\mathbf{g} \in \mathcal{V} + \mathbb{Z}^4$. The $\mathsf{Rec}(\mathbf{x}, \mathbf{r})$ is defined as follows:

$$\mathsf{Rec}(\mathbf{x}, \mathbf{r}) := \mathsf{Decode}\Big(\frac{1}{q}\mathbf{x} - \frac{q}{2^r}\mathbf{Br}\Big)$$

Protocol 1: NewHope

Alice		Bob
$\mathsf{seed} \overset{\$}{\leftarrow} \{0,1\}^{256}$		
$a \leftarrow \mathsf{Parse}(\mathsf{SHAKE\text{-}128}(\mathsf{seed}))$		
$s, e, \overset{\$}{\leftarrow} \Psi_{16}^n$		$s', e', e'' \overset{\$}{\leftarrow} \Psi_{16}^n$
	$\xrightarrow{(b,\mathsf{seed})}$	$a \leftarrow \mathsf{Parse}(\mathsf{SHAKE\text{-}128}(\mathsf{seed}))$
		$u \leftarrow as' + e'$
		$v \leftarrow bs' + e''$
$v' \leftarrow us$	$\xleftarrow{(u,r)}$	$r \overset{\$}{\leftarrow} \mathsf{HelpRec}(v)$
$\nu \leftarrow \mathsf{Rec}(v', r)$		$\nu \leftarrow \mathsf{Rec}(v, r)$
$\mu \leftarrow \mathsf{SHA3\text{-}256}(\nu)$		$\mu \leftarrow \mathsf{SHA3\text{-}256}(\nu)$

Parameters of NewHope are $n = 1024$ and $q = 12289$. They use binomial distribution is error sampling Ψ_{16}^n.

4.1.2 Frodo

Bos *et al.*[3] proposed LWE key exchange protocol called Frodo in 2016. Protocol 1 describes key exchange protocol of Frodo. To compute Frodo, we define $\mathsf{rec}()$, rounding, and cross-rounding functions.

Let the number B of bits that from one coefficient in $\mathcal{Z}_q$ be such that $B < (\log_2 q) - 1$. Let $\overline{B} = (\log 2q) - B$. The rounding function $\lfloor\cdot\rceil_{2^B}$ is defined as follows:

$$\lfloor\cdot\rceil_{2^B} : v \mapsto \left\lfloor 2^{-\overline{B}} v \right\rceil \mod 2^B$$

The cross-rounding function $\langle\cdot\rangle_{2^B}$ is defined as follows:

$$\langle\cdot\rangle_{2^B} : v \mapsto \left\lfloor 2^{-\overline{B}+1} v \right\rfloor \mod 2$$

Then, we can define $\mathsf{rec}()$ function as follows:

$$\mathsf{rec}(w, \langle v\rangle_{2^B}) := \lfloor v\rceil_{2^B} \quad if \quad |v - w| < 2^{\overline{B}-2}$$

Protocol 2: Frodo

Alice		Bob
$\mathsf{seed}_{\mathbf{A}} \xleftarrow{\$} U(\{0,1\}^s)$		
$\mathbf{A} \leftarrow \mathsf{Gen}(\mathsf{seed}_{\mathbf{A}})$		
$\mathbf{S}, \mathbf{E} \xleftarrow{\$} \chi(\mathbb{Z}_q^{n\times\overline{n}})$		
$\mathbf{B} \leftarrow \mathbf{AS} + \mathbf{E}$	$\xrightarrow[\in\{0,1\}^s\times\mathbb{Z}_q^{n\times\overline{n}}]{\mathsf{seed}_{\mathbf{A}},\mathbf{B}}$	$\mathbf{A} \leftarrow \mathsf{Gen}(\mathsf{seed}_{\mathbf{A}})$
		$\mathbf{S}', \mathbf{E}' \xleftarrow{\$} \chi(\mathbb{Z}_q^{n\times\overline{n}})$
		$\mathbf{B}' \leftarrow \mathbf{S}'\mathbf{B} + \mathbf{E}''$
		$\mathbf{C} \leftarrow \langle \mathbf{V} \rangle_{2^B}$
	$\xleftarrow[\in\mathbb{Z}_q^{\overline{m}\times n}\times\mathbb{Z}_2^{\overline{m}\times\overline{n}}]{\mathbf{B}'\mathbf{C}}$	
$K \leftarrow \mathsf{rec}(\mathbf{B}'\mathbf{S}, \mathbf{C})$		$K \leftarrow \lfloor \mathbf{V} \rceil_{2^B}$

There are 4 kinds of parameter sets in Frodo such as Challenge, Classical, Recommended, and Paranoid. In OQS library (liboqs) and this paper, we test recommended parameter set. Parameters of Frodo are $n = 752, q = 2^{15}, B = 4$. They use rounded Gaussian distribution is error sampling χ.

4.1.3 BCNS

Bos *et al.*[4] proposed Ring-LWE key exchange protocol called BCNS in 2015. Protocol 2 describes key exchange protocol of BCNS. To compute BCNS, we define $\mathsf{dbl}()$, $\mathsf{rec}()$, modular rounding, and cross-rounding functions. Let $\lfloor\cdot\rceil : \mathbf{R} \leftarrow \mathbb{Z}$ be the $\lfloor x \rceil = z$ for $z \in \mathbb{Z}$ and $x \in [z - 1/2, z + 1/2)$. The modular rounding function $\lfloor\cdot\rceil_{q,2}$ is defined as follows:

$$\lfloor\cdot\rceil_{q,2} : \mathbb{Z} \leftarrow \mathbb{Z}, \quad x \mapsto \lfloor x \rceil_{q,2} = \left\lfloor \frac{2}{q} x \right\rceil \mod 2$$

The cross-rounding function $\langle\cdot\rangle_{q,2}$ is defined as follows:

$$\langle\cdot\rangle_{q,2} : \mathbb{Z} \leftarrow \mathbb{Z}, \quad x \mapsto \langle\cdot\rangle_{q,2} = \left\lfloor \frac{4}{q} x \right\rceil \mod 2$$

Let $\mathsf{dbl}()$: $\mathbb{Z}_q \leftarrow \mathbb{Z}_{2q}$, $x \longmapsto \mathsf{dbl}(x) = 2x - e$, where e is sampled from $\{-1, 0, 1\}$ with probabilities $p_{-1} = p_1 = \frac{1}{4}$ and $p_0 = \frac{1}{2}$.

Define the sets $I_0 = \{-, 1, \cdots, \lfloor \frac{2}{q} \rceil - 1\}$ and $I_0 = \{-\lfloor \frac{q}{2} \rfloor, \cdots, -1\}$. Let $E = [-\frac{q}{4}, \frac{q}{4})$ the reconciliation function $\mathsf{rec}()$ function as follows:

$$\mathsf{rec}(w, b) = \begin{cases} 0 & \text{if } w \in I_b + E \mod 2q \\ 1 & \text{otherwise} \end{cases}$$

Protocol 3: BCNS

Alice		Bob
$s, e \xleftarrow{\$} \chi$		$s', e' \xleftarrow{\$} \chi$
$b \leftarrow as + e \in \mathcal{R}_q$	$\xrightarrow{b}$	$b' \leftarrow as' + e' \in \mathcal{R}_q$
		$e'' \xleftarrow{\$} \chi$
		$v \leftarrow bs' + e'' \in \mathcal{R}_q$
		$\overline{v} \xleftarrow{\$} \mathsf{dbl}(v) \in \mathcal{R}_{2q}$
	$\xleftarrow{b',c}$	$c \leftarrow \langle \overline{v} \rangle_{2q,2} \in \{0,1\}^n$
$k_A \leftarrow \mathsf{rec}(2b's, c) \in \{0,1\}^n$		$k_B \leftarrow \lfloor \overline{v} \rceil_{2q,2} \in \{0,1\}^n$

Parameters of BCNS are $n = 1024, q = 2^{32} - 1, \sigma = 8/\sqrt{2\pi} \approx 3.192$. They use discrete Gaussian distribution is error sampling χ.

4.1.4 MSrln

Longa *et al.*[6] proposed Ring-LWE key exchange protocol called MSrln in 2016. They suggest modular reduction technique using Montgomery reduction. Number Theoretic Transform (NTT) is used in polynomial multiplication and addition operations. Key exchange protocol scheme is same as NewHope protocol. Also, they use same parameters from NewHope key exchange protocol.

4.1.5 Kyber

Bos *et al.*[7] proposed Module-LWE key exchange protocol called Kyber in 2017. Protocol 4 describes key exchange protocol of Kyber. To compute Kyber, we define $\mathsf{Compress}()_q$ and $\mathsf{Decompress}()_q$ functions. Let $x \in \mathbb{Z}_q$ and $d < \lceil \log 2(q) \rceil$. The $\mathsf{Compress}()_q$ function is defined as follows:

$$\mathsf{Compress}()_q(x, d) = \lceil (2^d/q) \cdot x \rfloor \mod {}^{+}2^d$$

The $\mathsf{Decompress}()_q$ is defined as follows:

$$\mathsf{Decompress}()_q(x, d) = \lceil (q/2^d) \cdot x \rfloor$$

The $\mathsf{Enc}(pk, m)$ function is defined as follows:

$$\begin{aligned} \mathsf{Enc}(pk, m) &= (\mathbf{u}, v) \\ \mathbf{u} &= \mathsf{Compress}_q(\mathbf{A}^T r + \mathbf{e}_1, d_u) \\ v &= \mathsf{Compress}_q(\mathbf{t}^T r + e_2 + \left\lceil \frac{q}{2} \right\rceil \cdot m, d_v) \end{aligned}$$

$where, \mathbf{t} = \mathsf{Decompress}_q(\mathbf{t}, d_t), (r, \mathbf{e}_1, e_2) \in \beta_\eta^k \times \beta_\eta^k \times \beta_\eta$

The $\mathsf{Dec}(sk, (u, v))$ function is defined as follows:

$$\mathsf{Dec}(sk, (u, v)) = \mathsf{Compress}_q(v - \mathbf{s}^T \cdot \mathbf{u}, 1)$$

$where, \mathbf{u} = \mathsf{Decompress}_q(v, d_v), v = \mathsf{Decompress}_q(u, d_u)$

Protocol 4: Kyber

Alice		Bob
$\rho, \sigma \leftarrow \{0,1\}^{256}$		
$\mathbf{A} \leftarrow \mathsf{Sam}(\rho) \in \mathcal{R}_q^{k\times k}$		$m \leftarrow \{0,1\}^{256}$
$(\mathbf{s}, \mathbf{e}) \leftarrow \mathsf{Sam}(\sigma) \in \beta_\eta^k \times \beta_\eta^k$		$(\hat{K}, r, d) \leftarrow G((\mathbf{t}, \rho), m)$
$\mathbf{t} \leftarrow \mathsf{Compress}_q(\mathbf{As} + \mathbf{e}, d_t)$	$\xrightarrow{(\mathbf{t},\rho)}$	$(\mathbf{u}, v) \leftarrow \mathsf{Enc}((\rho, \mathbf{t}), m; r))$
		$c \leftarrow (\mathbf{u}, v, d)$
	$\xleftarrow{c}$	
$m' \leftarrow \mathsf{Dec}(\mathbf{s}, (\mathbf{u}, v))$		
$(\hat{K}', r', d') \leftarrow G(pk, m')$		
$(\mathbf{u}', v') \leftarrow \mathsf{Enc}((\rho, \mathbf{t}), m'; r')$		$K \leftarrow H(c, K)$
$(\mathbf{u}', v', d') = (\mathbf{u}, v, d);$		
$K \leftarrow H(\hat{K}', c)$		
$(\mathbf{u}', v', d') \neq (\mathbf{u}, v, d);$		
$K \leftarrow H(z, c)$		

Table 2: Payload on Open Quantum Safe Protocol

Mathematical Problem	Protocol	Payload (byte)			
		Alice → Bob	Bob → Alice	Total Payload	Session Key Size
Lattice-based	Frodo	11280	11288	22568	32
	BCNS	4096	4224	8320	128
	NewHope	1824	2048	3872	32
	MSrln	1824	2048	3872	32
	Kyber	1088	1184	2272	32
	NTRU	1027	1022	2049	32
Code-based	McBits	311736	141	311877	32
Supersingular Isogeny Elliptic Curve	IQC	1164	1164	2328	194
	MSR SIDH	1164	1164	2328	194

Parameters of Kyber are $n = 256, q = 7681, k = 3, \eta = 4, d_u = 11, d_v = 3, d_t = 11$. They use binomial distribution is error sampling β_η^k. $H()$ and $G()$ are cryptographic hash functions.

There is 3 version of key exchange protocol such as unauthenticated, one-sided authenticated, and authenticated. Protocol 4 describes unauthenticated key exchange protocol using Kyber.

4.2 Performance Test

In this section, we show detail results of liboqs such as payload and runtime.

4.2.1 Experimental Setup

The experimental environment is as follows: Intel(R) CPU i7-5500, RAM 16GB, and test on Ubuntu v16.04. The compiler also uses gcc v5.4.0. We download reference liboqs source code in GitHub[1].

4.2.2 Performance of liboqs

Table 2 describes payload of OQS project. NTRU has smallest total payload as 2049-byte. Ring-LWE and SIDH key exchange protocols have a smaller payload than code-based protocol. The largest payload in the table is McBits, which is 311877-byte. We also check payload of LWE scheme is larger than Ring-LWE scheme. Because Ring-LWE computes ring structure. Therefore, Ring-LWE is efficient than LWE scheme. Especially, in case of McBits, since the payload of Alice → Bob is about 0.3MB. Therefore, McBits can be utilized in the IoT device when Server has high computational power. The size of the shared key between the server and the client is 32-bit, 128-bit or 194-bit. Session key of supersingular isogeny elliptic curve is 194-bit. In Alice to Bob's payload has the largest McBit as 311736-byte and the smallest NTRU as 1027-byte. In Bob to Alice's payload has the largest Frodo as 11288-byte and the smallest McBits as 141-byte. As a result of combining both payloads, the largest payload is McBits as 311877-byte and the smallest payload is NTRU as 2049-byte.

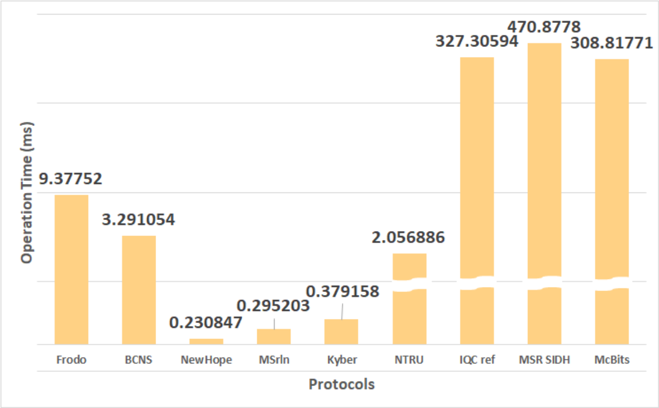

Figure 1: Comparing Runtime of OQS Protocols

Figure 1 shows runtime of OQS protocols. NewHope, MSrln, and Kyber based on Ring-LWE scheme are faster than other protocols. Runtime of NewHope is about 0.23ms and Kyber is 0.38ms. However, total runtime of supersingular Isogeny Elliptic Curves such as IQC and MSR SIDH are at least 300ms. McBits has almost same result in SIDH schemes. These three kinds of schemes are about 10 times slower than Ring-LWE schemes. The fastest key exchange protocol is NewHope, which takes 0.23ms. However, The slowest key exchange protocol is MSR SIDH, which takes 470.88ms.

Figure 2 shows detail runtime of lattice-based OQS protocols. Red line means total runtime of the protocol. First Alice pre-computation (Alice Comp. 0) phase initiates key exchange protocol. Bob receives Alice's payload, Bob computes shared key (Bob Comp.). Then, Alice computes shared key(Alice Comp. 1). Frodo is slowest key exchange protocol more than 3ms in Alice Comp. 0 and Bob Comp. . Because Frodo uses LWE scheme for security reason. However, LWE is slower than Ring-LWE schemes. NewHope, MSrln, and Kyber consume less than 1ms in all phase.

[1] https://github.com/open-quantum-safe/liboqs

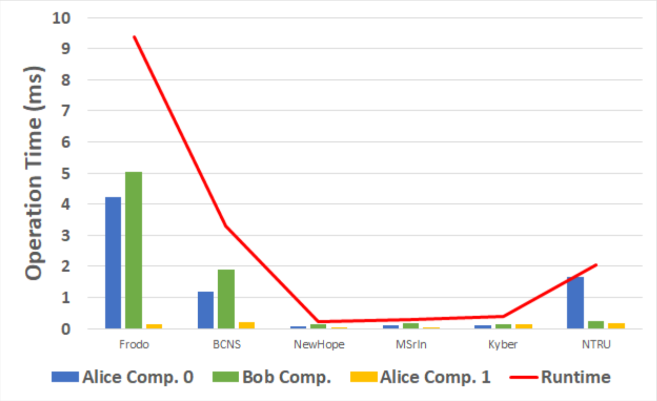

Figure 2: Runtime of Lattice-based Protocol

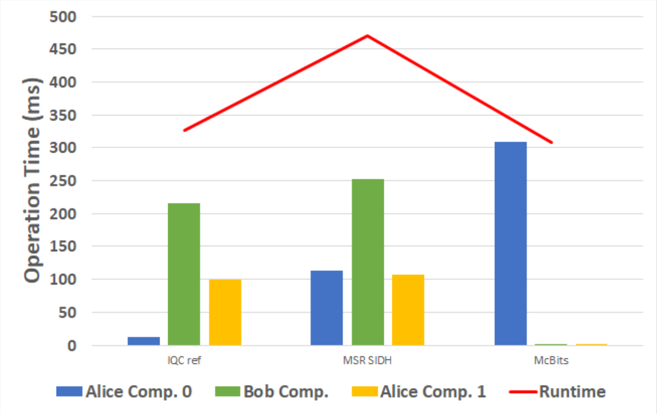

Figure 3: Runtime of Code-based and SIDH Protocols

Figure 3 shows runtime of code-based and SIDH protocols. SIDH schemes take more than 100ms in Bob Comp. phase. In the case of McBits takes more than 300ms in Alice Comp. 0 phase. The protocol with the longest computation time is 45 ms in MSR SIDH. As a result of comparing IQC and MSR SIDH, SIDH schemes are effective to use IQC with short (Alice Comp. 0) operation time. Compared with a result of Figure 2, the total operation time is about 30 times longer.

5 Conclusion and Future Work

In this paper, we introduce Open Quantum Safe project which is quantum-resistant key exchange protocols. OQS project consists of lattice-based, code-based, and supersingular Isogeny elliptic curve. There are 6 kinds of key exchange protocol in lattice-based cryptography such as Frodo, BCNS, NewHope, MSrln, and Kyber. In supersingular isogeny elliptic curve has two kinds of schemes such as IQC and MSR SIDH. Finally, the code-based scheme is McBits. We introduce and describe lattice-based key exchange schemes. Key exchange protocol of liboqs can replace classical protocol such as Elliptic Curve Diffie-Hellman (ECDH). We experiment liboqs protocol as payload and runtime. As a result, lattice-based key exchange protocols is practical approach.

As future work, we will merge into Public Key Infrastructure (PKI) system. Current PKI system is not secure against quantum computing attacks. However, key exchange protocols in liboqs are quantum-resistant algorithms. Using quantum-resistant key exchange protocol, we can add a lot of applications such as voting, smart contract, and smart meter protocols. We will write OQS project part II paper. In part II paper, we will describe the background of SIDH and code-based key exchange schemes. We will check detailed McBits, IQC, and MSR SIDH key exchange protocol.

Acknowledgements

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00555, Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World) and National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2015R1A2A2A01006812, Design and Security Analysis of Novel Lattice-based Fully Homomorphic Signatures Robust to Quantum Computing Attack).

References

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings, Annual Symposium on Foundations of Computer Science–FOCS'94*, pp. 124–134, IEEE, 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing–STOC'96*, pp. 212–219, ACM, 1996.

[3] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the ring! practical, quantum-secure key exchange from LWE," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security–ACM CCS'16*, pp. 1006–1018, ACM, 2016.

[4] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *IEEE Symposium on Security and Privacy–IEEE S&P'16*, pp. 553–570, IEEE, 2015.

[5] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—a new hope," in *USENIX Security Symposium–USENIX Security'16*, pp. 327–343, 2016.

[6] P. Longa and M. Naehrig, “Speeding up the number theoretic transform for faster ideal lattice-based cryptography,” in *in International Conference on Cryptology And Network Security–CANS'16*, pp. 124–139, Springer, 2016.

[7] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé, “CRYSTALS–Kyber: a CCA-secure module-lattice-based KEM,” in *Cryptology ePrint Archive, Report 2017/634*, 2017. http://eprint.iacr.org/2017/634.

[8] J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A ring-based public key cryptosystem,” in *International Algorithmic Number Theory Symposium–ANTS'98*, pp. 267–288, Springer, 1998.

[9] D. J. Bernstein, T. Chou, and P. Schwabe, “McBits: fast constant-time code-based cryptography,” in *in Conference on Cryptographic Hardware and Embedded Systems–CHES'13*, pp. 250–272, Springer, 2013.

[10] D. Jao and L. De Feo, “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.,” *International Workshop on Post-Quantum Cryptography–PQCrypto'11*, vol. 7071, pp. 19–34, 2011.

[11] C. Costello, P. Longa, and M. Naehrig, “Efficient algorithms for supersingular isogeny diffie-hellman,” in *Annual International Cryptology Conference on Advances in Cryptology–CRYPTO'16*, pp. 572–601, Springer, 2016.

[12] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” *Journal of the ACM (JACM)*, vol. 56, no. 6, p. 34, 2009.

[13] V. Lyubashevsky, C. Peikert, and O. Regev, “On ideal lattices and learning with errors over rings,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques–EUROCRYPT'10*, pp. 1–23, Springer, 2010.

[14] A. Langlois and D. Stehlé, “Worst-case to average-case reductions for module lattices,” *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

[15] J. Ding, X. Xie, and X. Lin, “A simple provably secure key exchange scheme based on the learning with errors problem,” in *Cryptology ePrint Archive, Report 2012/688*, 2012. http://eprint.iacr.org/2012/688.

[16] C. Peikert, “Lattice cryptography for the internet,” in *International Workshop on Post-Quantum Cryptography–PQCrypto'14*, pp. 197–219, Springer, 2014.

[17] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, “Authenticated key exchange from ideal lattices.,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques–EUROCRYPT'15*, pp. 719–751, 2015.

[18] H. Krawczyk, “HMQV: A high-performance secure diffie-hellman protocol (extended abstract),” in *Annual International Cryptology Conference on Advances in Cryptology–CRYPTO'05*, pp. 546–566, Springer, 2005.

[19] S. M. Bellovin and M. Merritt, “Encrypted key exchange: Password-based protocols secure against dictionary attacks,” in *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on –IEEE S&P'92*, pp. 72–84, IEEE, 1992.

[20] J. Katz and V. Vaikuntanathan, “Smooth projective hashing and password-based authenticated key exchange from lattices.,” in *Annual International Conference on the Theory and Applications of Cryptology and Information Security–ASIACRYPT'09*, vol. 5912, pp. 636–652, Springer, 2009.

[21] J. Zhang and Y. Yu, “Two-round pake from approximate sph and instantiations from lattices,” in *Annual International Conference on the Theory and Applications of Cryptology and Information Security–ASIACRYPT'17*, pp. 37–67, Springer, 2017.

[22] J. Ding, S. Alsayigh, J. Lancrenon, R. Saraswathy, and M. Snook, “Provably secure password authenticated key exchange based on RLWE for the post-quantum world,” in *Proceedings of Cryptographers Track RSA Conference–CT-RSA'17*, pp. 183–204, Springer, 2017.

[23] D. Xu, D. He, K.-K. R. Choo, and J. Chen, “Provably secure three-party password authenticated key exchange protocol based on ring learning with error,” in *Cryptology ePrint Archive, Report 2017/360*, 2016. http://eprint.iacr.org/2017/360.

[24] D. Stebila and M. Mosca, “Post-quantum key exchange for the internet and the open quantum safe project,” in *Cryptology ePrint Archive, Report 2016/1017*, 2016. http://eprint.iacr.org/2016/1017.