CLOQS 라이브러리 가이드

1. **CLOQS** 라이브러리 소개

이 라이브러리는 NIST에서 표준으로 채택한 3종의 PQC 알고리즘과 KPQC(HAETAE, AIMer, NTRU+, SMAUG-T)을 모두 통합한 범용 암호 라이브러리입니다.
이 라이브러리는 C, Java, JavaScript 언어를 모두 지원하며, Linux 및 Windows 환경에서 호환됩니다.

최신 릴리스는 아래 주소에서 다운로드할 수 있습니다.
CLOQS Drive

2. Kem 알고리즘

2.1 ML-KEM

- 알고리즘 유형: 키 캡슐화 메커니즘 (KEM)
- 주요 암호학적 가정 : Module-LWE, over $\mathbb{Z}[x]/(3329, x^{256} + 1)$

2.1.1 소스 및 라이선스

- 주 소스: mlkem-native GitHub
- 라이선스 : CC0-1.0 또는 Apache-2.0

2.1.2 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	캡슐화 크기 **(B)**	공유 비밀 크기 **(B)**
ML-KEM-512	IND-CCA2	1	800	1632	768	32
ML-KEM-768	IND-CCA2	3	1184	2400	1088	32
ML-KEM-1024	IND-CCA2	5	1568	3168	1568	32

2.2 SMAUG-T

- 알고리즘 유형 : 키 캡슐화 메커니즘 (KEM)
- 주요 암호학적 가정 : Module-LWE + Module-LWR, over $\mathbb{Z}[x]/(q, x^{256} + 1)$, q=1024 or 2048

2.2.1 소스 및 라이선스

- 주 소스 : SMAUG-T Github
- 라이선스 : MIT License

2.2.2 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	캡슐화 크기 **(B)**	공유 비밀 크기 **(B)**
SMAUG-T128	IND-CCA2	1	832	672	672	32
SMAUG-T192	IND-CCA2	3	1312	1088	992	32
SMAUG-T256	IND-CCA2	5	1728	1440	1376	32

2.3 NTRU+

- 알고리즘 유형 : 키 캡슐화 메커니즘 (KEM)
- 주요 암호학적 가정 : NTRU, over $\mathbb{Z}[x] / (3457, x^n - x^{n/2} + 1)$

2.3.1 소스 및 라이선스

- 주 소스 : NTRU+ Github
- 라이선스 : MIT License

2.3.2 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	캡슐화 크기 **(B)**	공유 비밀 크기 **(B)**
NTRUPLUS-KEM-576	IND-CCA2	1	864	1760	864	32

NTRUPLUS-KEM-768	IND-CCA2	1	1152	2336	1152	32
NTRUPLUS-KEM-864	IND-CCA2	3	1296	2624	1296	32
NTRUPLUS-KEM-1152	IND-CCA2	5	1728	3488	1728	32

3. Sig 알고리즘

3.1 ML-DSA

- 알고리즘 유형 : 디지털 서명 알고리즘 (Digital Signature Scheme)
- 주요 암호학적 가정 : Module-LWE + Module-SIS, over $\mathbb{Z}[x]/(8380417, x^{256} + 1)$

3.1.1 소스 및 라이선스

- 주 소스 : pq-crystals GitHub
- 라이선스 : CC0-1.0 또는 Apache-2.0

3.1.2 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	서명 크기 **(B)**
ML-DSA-44	SUF-CMA	2	1312	2560	2420
ML-DSA-65	SUF-CMA	3	1952	4032	3309
ML-DSA-87	SUF-CMA	5	2592	4896	4627

3.2 SPHINCS+

- 알고리즘 유형 : 디지털 서명 알고리즘 (Digital Signature Scheme)
- 주요 암호학적 가정 : Collision-Resistance + Second Preimage-Resistance of SHA2 or SHAKE

3.2.1 소스 및 라이선스

- 주 소스 : PQClean GitHub
- 라이선스 : CC0-1.0

3.2.2 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	서명 크기 **(B)**
SPHINCS+-SHA2-128f-simple	EUF-CMA	1	32	64	17088
SPHINCS+-SHA2-128s-simple	EUF-CMA	1	32	64	7856
SPHINCS+-SHA2-192f-simple	EUF-CMA	3	48	96	35664
SPHINCS+-SHA2-192s-simple	EUF-CMA	3	48	96	16224
SPHINCS+-SHA2-256f-simple	EUF-CMA	5	64	128	49856
SPHINCS+-SHA2-256s-simple	EUF-CMA	5	64	128	29792
SPHINCS+-SHAKE-128f-simple	EUF-CMA	1	32	64	17088

SPHINCS+-SHAKE-128s-simple	EUF-CMA	1	32	64	7856
SPHINCS+-SHAKE-192f-simple	EUF-CMA	3	48	96	35664
SPHINCS+-SHAKE-192s-simple	EUF-CMA	3	48	96	16224
SPHINCS+-SHAKE-256f-simple	EUF-CMA	5	64	128	49856
SPHINCS+-SHAKE-256s-simple	EUF-CMA	5	64	128	29792

3.3 HAETAE

- 알고리즘 유형 : 디지털 서명 알고리즘 (Digital Signature Scheme)
- 주요 암호학적 가정 : Module-LWE + Module-SIS, over $\mathbb{Z}[x]/(64513, x^{256} + 1)$

3.3.1 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	서명 크기 **(B)**
HAETAE2	EUF-CMA	2	992	1408	1474
HAETAE3	EUF-CMA	3	1472	2112	2349
HAETAE5	EUF-CMA	5	2080	2752	2948

3.4 Aimer

- 알고리즘 유형 : 디지털 서명 알고리즘 (Digital Signature Scheme)
- 주요 암호학적 가정 : MPC-in-the-Head (MPCitH) + One-wayness of "AIM" symmetric primitive

3.4.1 소스 및 라이선스

- 주 소스 : Samsungsds AIMer GitHub
- 라이선스 : MIT License

3.4.2 파라미터 세트 요약

파라미터 세트	보안 모델	**NIST** 보안 수준	공개키 크기 **(B)**	비밀키 크기 **(B)**	서명 크기 **(B)**
AIMER128S	EUF-CMA	1	32	48	4160
AIMER128F	EUF-CMA	1	32	48	5888
AIMER192S	EUF-CMA	3	48	72	9120
AIMER192F	EUF-CMA	3	48	72	13056
AIMER256S	EUF-CMA	5	64	96	17056
AIMER256F	EUF-CMA	5	64	96	25120