양자내성암호 국가공모전[KpqC 공모전]

(Korean Post-Quantum Cryptography Competition)

1라운드 알고리즘 제출 안내

1. KpqC 공모전 1라운드 알고리즘 제출 안내

KpqC 공모전에 '개발 계획서'가 채택되어 알고리즘 설계를 진행하고 계신 개발자분들에게 1라운드 알고리즘 제출에 관해 다음과 같이 안내해드립니다.

❍ 제출 기한: 2022년 10월 31일(월)

❍ 제출 방법: 이메일(kpqcrypto@gmail.com)로 제출

❍ 제출물 목록

- 알고리즘 제안서
- 참조(reference) 구현 코드 및 KAT(Known Answer Test) 값

※ 제출물은 홈페이지(www.kpqc.or.kr)를 통해 공개될 예정입니다.

❍ 문의: 이메일 kpqcrypto@gmail.com

❍ [첨부1] 향후 주요 일정

[첨부2] 참고용 '알고리즘 제안서' 양식

[첨부3] 라이선스 정보 샘플

2. 제출물 작성 안내

❍ 알고리즘 제안서

- 작성 언어: 영문
- 제출 형식: pdf

※ [첨부2]는 참고용 양식으로 목차, style 등의 수정이 가능합니다.

- '개발 계획서' 관련 고려사항
  - '개발 계획서'의 내용을 '알고리즘 제안서'에서 변경할 수 있는 범위에

대해 정해진 사항은 없으며, 소수의 참여자 변경을 포함한 연구 과정에서 통상적으로 일어날 수 있는 정도의 변경은 자유롭게 반영하실 수 있습니다.

- 다만, 변경의 정도가 크거나, 대상이 특이하여 논란의 여지가 있다고 판단되시는 사항에 대해서는 연구단 간사와 사전에 협의 부탁드립니다.

- 포함 내용[1)]
  - 알고리즘 명
  - KpqC 공모전 제출 명시 문구 ([첨부2] 참조)
  - 알고리즘 설계 사상, 장단점 등의 주요 특징
  - 알고리즘 상세 규격(specification)
  - 구성 요소(비밀키, 공개키, 암호문, 서명 값 등)의 크기
  - 참조 구현 성능
  - 안전성 정의에 대한 증명('개발 계획서' 양식의 참고사항 2.가. 참조)
  - 정량적 안전성과 그 근거('개발 계획서' 양식의 참고사항 2.나. 참조)
  - 기존 공격에 대한 안전성 분석 결과

- '알고리즘 제안서'는 제출과 함께 IACR Cryptology ePrint Archive 또는 잘 알려진 국제 학회, 국제 저널에 게재하는 것을 의무로 합니다.

> 게재 문서에 KpqC 공모전(홈페이지 주소 포함)에 제안된 알고리즘 관련 연구 결과임을 자유로운 방식(예를 들어, 참고문헌, 각주 등)으로 명시 부탁드리며, ePrint는 22년 11월, 학회/저널은 23년 8월을 게재 기한으로 하고자 합니다.

❍ 참조 구현 코드 및 KAT 값

> 작성 프로그래밍 언어, 구현 API(Application Programming Interface), KAT 값 생성 방법 등은 개발의 편의성, 국제적인 활용성 및 검증 효율성 등을 위하여 보편적으로 사용되고 있는 NIST 공모전 양식[2)]을 따르고자 합니다.

- 작성 프로그래밍 언어: ANSI C
- 알고리즘 참조(reference) 구현

1) '알고리즘 제안서'의 권장 포함 내용으로, 알고리즘을 정확히 설명하고, 우수성을 강조하는데 필요한 경우 일부 변경이 가능합니다.

2) csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/example-files

- 위 참조의 API Notes에서 알고리즘 기능에 따라 제공하는 방식으로 구현
  예) KEM은 crypto_kem_keypair(), crypto_kem_enc(), crypto_kem_dec() 세 개의 함수를 API 형식에 따라 입출력을 처리할 수 있도록 구현

- KAT(Known Answer Test) 값 생성

※ 알고리즘을 새롭게 구현했을 경우, 정확하게 구현되었는지 확인하기 위해 KAT 값이 필요함

- 위 참조에서 제공하는 KAT 값 계산 스크립트로 생성한 파일 제출
  예) KAT 값은 REQUEST(.req)와 RESPONSE(.rsp) 2개의 파일로 구성됨(.req 파일에는 랜덤한 48바이트 seed 값 100개가 저장되며, KEM의 경우 .rsp 파일에는 100개의 공개키, 비밀키, 암호문, 공유키[3] 쌍이 저장됨)

- 라이선스 정보

- 제출된 구현물은 연구단 홈페이지를 통해 공개될 예정이므로, 구현 코드에 대하여 필요한 license 조항을 제출물에 포함하는 것을 권장합니다.

※ 예를 들어, 'MIT license(MIT)[4]' 의 적용이 필요하신 경우 [첨부3]에 연도와 저작권 소유자를 기재하여 제출하시면 됩니다.

❍ 제출 관련 세부 사항

- 제출 메일의 본문에 다음 사항을 작성 부탁드립니다.

- 외부 게재/투고 정보
- '개발 계획서' 대비 추가되거나 정보가 변경된 개발자의 정보(이름, 소속, 이메일, 전화번호)

- 아래와 같이 구성한 제출물을 (알고리즘명).zip으로 압축하여 메일에 첨부

- \license.txt
- \document\(알고리즘명).pdf ('알고리즘 제안서')
- \reference_implementation*.* (참조 구현 코드가 포함된 파일들)
- \KAT*.* (KAT 값 포함 *.req, *.rsp 파일)

3) .req 파일에서 seed를 읽어 난수 생성 초기값으로 사용하고, keypair 함수로 공개키, 비밀키를, enc 함수로 암호문, 공유키를 각각 생성하고, dec 함수로 다시 생성한 공유키가 일치하는지 확인 후 저장함
4) 한국저작권위원회 '오픈소스SW라이선스 종합정보시스템(olis.or.kr)'에서 관련 정보 확인 가능

3. 평가 기준

제안된 알고리즘은 아래의 기준을 중심으로 평가될 예정입니다.

- 안전성(안전성 정의에 대한 증명, 정량적 안전성에 대한 근거 등)
- 효율성(구성 요소의 크기, 복호화 실패 확률, 참조 구현 동작 효율성 등)
- 다양한 환경에서의 활용성
- 독창성, 기반 문제 신뢰성 등의 알고리즘 특징

[첨부1]

KpqC 공모전 향후 주요 일정

시기	내용	
< KpqC 공모전 1라운드 >		
’22. 11. 24.~25.	2022 KpqC 5차 워크숍	1라운드 알고리즘 발표
’23. 7./11.	2023 KpqC 6/7차 워크숍	알고리즘 분석/개선 결과 공유
’23. 12.	공모전 1라운드 결과 발표	2라운드 후보 목록 공개
’24. 2.	‘2라운드 알고리즘’ 접수 마감	
< KpqC 공모전 2라운드 >		
’24. 3.	2024 KpqC 8차 워크숍	2라운드 알고리즘 발표
’24. 9.	2024 KpqC 9차 워크숍	알고리즘 분석/개선 결과 공유
	KpqC 공모전 최종 결과 발표	알고리즘 ○종 선정 예정

※ 관련 일정은 진행 상황에 따라 변경될 수 있습니다.

[첨부2]

Title including the algorithm name*

First Author[1], Second Author[2], and Third Author[2]

[1] Institute 1
fa@institute1mail.com
[2] Institute 2
sa,ta@institute2mail.com

Abstract. The abstract should briefly summarize the contents of the paper.

Keywords: First keyword · Second keyword · Another keyword.

1 Introduction

Introductory contents...
A citation sample [1].

1.1 Design rationale

design rationale

1.2 Advantages and limitations

advantages and limitations

2 Preliminaries

background and/or related previous works

* This work is submitted to 'Korean Post-Quantum Cryptography Competition' (www.kpqc.or.kr).

3 Specification

specification of the algorithm

3.1 Notation

required notations for specification

3.2 Specification of (ALGORITHM NAME)

specification using algorithms and subroutines

3.3 Parameter sets

parameter sets and derived constants(size of private, public key and ciphertext or signature)

4 Performance analysis

performance analysis of the algorithm

4.1 Description of platform

platform description

4.2 Performance of reference implementation

performance of implementation

5 Security

security of the algorithm

5.1 Security definition

security definition with proof

5.2 Security strength categories

security categories by quantitative estimates

5.3 Cost of known attacks

cost of known attacks

Description and cost of (the first attack) description of (the first attack) and cost analysis

Description and cost of (the second attack) description of (the second attack) and cost analysis

6 Summary or Conclusion

summary or conclusion of this work

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review **41**(2), 303–332 (1999)

A Title of appendix section

appendix contents (if exists)

[첨부3]