Draft

국가·공공기관

# 암호 안전성 기준

양자컴퓨팅 시대 안전한 암호의 선택 지침서



CRYPTOGRAPHIC SECURITY
GUIDELINE

2026. 11.

국가정보원
NATIONAL INTELLIGENCE SERVICE

NSR
국가보안기술연구소

Draft

국가·공공기관

# 암호 안전성 기준

양자컴퓨팅 시대 안전한 암호의 선택 지침서

CRYPTOGRAPHIC SECURITY GUIDELINE

2026. 11.

**본 「국가 · 공공기관 암호 안전성 기준」 발간 과정에서 소중한 자문과 도움을 주신 분들께 깊이 감사드립니다.**

| | | | |
|---|---|---|---|
| 한국전자통신연구원 | 강유성 실장 | 국민대학교 | 염용진 교수 |
| 국민대학교 | 강주성 교수 | 이화여자대학교 | 윤아람 교수 |
| 아주대학교 | 곽진 교수 | 인하대학교 | 이문규 교수 |
| 국민대학교 | 김동찬 교수 | 순천향대학교 | 이임영 교수 |
| 한국인터넷진흥원 | 김준섭 팀장 | KAIST | 이주영 교수 |
| 부산대학교 | 김호원 교수 | 전북대학교 | 홍득조 교수 |
| 고려대학교 | 김희석 교수 | 드림시큐리티社 | 김대식 이사 |
| 세종대학교 | 노동영 교수 | 삼성SDS社 | 문덕재 수석 |
| 세종사이버대학교 | 박영호 교수 | NSHC社 | 윤기순 연구소장 |
| 한양대학교 ERICA | 서승현 교수 | | |

**[문서의 영향과 범위]**

이 문서는 국가정보원의 국가 암호기술 정책서 배포 계획에 의해 기획 · 작성 · 출판되었으며, 향후 국가 암호기술 사용 정책 및 암호모듈 검증제도(KCVMP) 등 제반 여건에 따라 개정될 수 있습니다.

이 문서의 내용은 국내외 학계, 산업계, 연구계가 축적한 지식을 바탕으로 국가정보원과 국가보안기술연구소가 수립한 가이드라인입니다. 이 문서 자체는 법적 강제력을 가지지 않으나, 별도 법 · 시행령 등에서 구속력 있는 의무화 지침으로 활용될 수 있습니다. 또한 의무화 지침으로 활용되지 않더라도 국가 · 공공기관 등에서 이 문서 전체 혹은 일부를 활용, 준수해야 할 보안 통제 수단 등의 기술적 기준으로 사용할 수 있습니다.

이 문서를 활용하여 중앙행정기관 및 그 소속기관, 지방자치단체 및 그 소속기관, 공공기관 및 국가 기반시설 운영기관 등이 안전한 정보보안 정책을 수립하고 정보시스템을 운영하는 과정에서 종합적인 기술적 기준으로 활용하기를 기대합니다.

**[이용 대상]**

이 문서는 주요 정보자산을 처리하거나 보호해야 하는 모든 국가기관과 공공기관을 대상으로 작성되었습니다. 특히 각 기관에서 보안 정책을 수립하거나, 보안 시스템을 기획, 도입, 운영하는 담당자, 그리고 보안 점검 및 대응 업무를 수행하는 실무자, 공공조달 기업체 등을 주요 대상으로 작성되었습니다.

**[저작권]**


- 국가정보원과 국가보안기술연구소와의 사전 협의 없이 문서의 전부 또는 일부를 상업적 목적으로 복제 및 배포 금지

- 비상업적 목적으로 문서 내용의 전부 또는 일부를 이용하고자 할 때는 반드시 출처 명기

**[제 · 개정 이력]**

| 개정일 | 버 전 | 내 역 | 비 고 |
|---|---|---|---|
| 2026.11. | Draft | 초안 출판 | |
| | | | |
| | | | |

# CONTENTS

국가·공공기관 **암호 안전성 기준**
CRYPTOGRAPHIC SECURITY GUIDELINE


**Chapter 01** 서론 1

**Chapter 02** 보안 강도 기준 수립 방침 7

제1절 암호의 보안 강도 8

제2절 보안 강도 기준 수립 고려 사항 12

**Chapter 03** 암호 알고리즘 사용 기준 21

제1절 국가·공공 암호 알고리즘 사용 기준 총괄 23

제2절 암호 보안 강도 기준 수립 원칙 24

**Chapter 04** 암호 알고리즘별 사용 정책 27

제1절 대칭 키 암호 28

제2절 비대칭 키 암호 40

제3절 비대칭 키 암호의 하이브리드 사용 46

■ 부록 49

1. 국내외 암호 정책 동향 50
2. 주요 암호기술 소개 66

■ 주요 용어 및 약어 83

1. 용어의 정의 84
2. 약어 88

■ 참고 문헌 91

## [표 차례]

[표 1] 양자컴퓨터를 고려한 국제 표준기구(ISO/IEC)의 암호 안전성 기준 10
[표 2] 국내외 암호 안전성 기준 관련 문서 13
[표 3] 암호 알고리즘 사용 형태에 관한 표현 22
[표 4] 암호 알고리즘 시기별 사용 정책에 관한 표현 22
[표 5] 암호 알고리즘 사용 기준 총괄 23
[표 6] 블록암호 알고리즘 보안 강도 기준 29
[표 7] 블록암호 운영모드 보안 강도 기준 30
[표 8] 해시함수 보안 강도 기준 31
[표 9] CMAC 보안 강도 기준 33
[표 10] GMAC 보안 강도 기준 33
[표 11] HMAC 보안 강도 기준 34
[표 12] 블록암호 기반 난수발생기(PRNG) 보안 강도 기준 35
[표 13] 해시함수 기반 난수발생기(PRNG) 보안 강도 기준 36
[표 14] CMAC 기반 키 유도 함수 알고리즘 보안 강도 기준 38
[표 15] HMAC 기반 키 유도 함수 알고리즘 보안 강도 기준 38
[표 16] 확장 출력 함수 보안 강도 기준 39
[표 17] 공개 키 암호화 알고리즘 보안 강도 기준 40
[표 18] 전자서명 RSASSA 보안 강도 기준 41
[표 19] 전자서명 KCDSA 보안 강도 기준 41
[표 20] 전자서명 알고리즘(타원곡선 기반) 보안 강도 기준 41
[표 21] 양자내성 전자서명 안전성 범주 기준 42



[표 22] 양자내성 전자서명 알고리즘 예시 42
[표 23] DH 키 합의 보안 강도 기준 44
[표 24] ECDH 키 합의 보안 강도 기준 44
[표 25] 양자내성 KEM 보안 강도 기준 45
[표 26] 양자내성 KEM 알고리즘 예시 45
[표 27] PQ/T 하이브리드의 보안 강도 및 안전성 범주 기준 46
[표 28] PQ/PQ 하이브리드의 안전성 범주 기준 47
[표 29] 미국의 암호 보안 강도 및 알고리즘 사용에 관한 정책 51
[표 30] 캐나다의 암호 보안 강도 및 알고리즘 사용에 관한 정책 52
[표 31] 유럽연합의 암호 보안 강도 및 알고리즘 사용에 관한 정책 55
[표 32] 독일의 암호 보안 강도 및 알고리즘 사용에 관한 정책 56
[표 33] 프랑스의 암호 보안 강도 및 알고리즘 사용에 관한 정책 58
[표 34] 네덜란드의 암호 보안 강도 및 알고리즘 사용에 관한 정책 59
[표 35] 영국의 암호 보안 강도 및 알고리즘 사용에 관한 정책 61
[표 36] 일본의 암호 보안 강도 및 알고리즘 사용에 관한 정책 62
[표 37] KCMVP 검증대상 블록암호 알고리즘 표준 목록 67
[표 38] KCMVP 검증대상 블록암호 운영모드 표준 목록 68
[표 39] KCMVP 검증대상 해시함수 알고리즘 표준 목록 69
[표 40] KCMVP 검증대상 메시지 인증코드 알고리즘 표준 목록 70
[표 41] KCMVP 검증대상 난수발생기(PRNG) 알고리즘 표준 목록 72
[표 42] KCMVP 검증대상 키 유도 함수 표준 목록 73
[표 43] 확장 출력 함수 알고리즘 표준 목록 74

[표 44] KCMVP 검증대상 공개 키 암호화 알고리즘 표준 목록 75
[표 45] KCMVP 검증대상 기존 전자서명 알고리즘 표준 목록 76
[표 46] 주요 양자내성 전자서명 알고리즘 예시 76
[표 47] KCMVP 검증대상 키 설정 알고리즘 표준 목록 78
[표 48] 주요 양자내성 KEM 알고리즘 예시 79
[표 49] 표준화가 진행 중인 하이브리드 방식 81

## [그림 차례]

[그림 1] 국내 비대칭 키 암호 사용 전환 로드맵 17
[그림 2] 블록암호 개념도 67
[그림 3] 블록암호 운영모드 개념도 68
[그림 4] 해시함수 개념도 69
[그림 5] 메시지 인증코드 개념도 70
[그림 6] 난수발생기 개념도 71
[그림 7] 키 유도 함수 개념도 72
[그림 8] 확장 출력 함수 개념도 73
[그림 9] 공개 키 암호화 개념도 75
[그림 10] 전자서명 개념도 76
[그림 11] 키 설정 개념도 77
[그림 12] 키 합의 개념도 78
[그림 13] KEM 개념도 79
[그림 14] 하이브리드 KEM 개념도 80
[그림 15] 하이브리드 전자서명 개념도 81

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



# Chapter 01
# 서 론

Chapter 01

# 서 론

국가 전반에 걸친 디지털 전환이 빠르게 진행됨에 따라 행정, 국방, 외교, 재난관리, 공공서비스 제공 등 국가·공공 분야의 다양한 업무를 정보시스템에 의존하여 수행하고 있다. 특히, 국가 정보통신망에는 국민의 개인정보뿐만 아니라 국가 기밀과 주요 정책 정보가 대량으로 유통되고 있어, 이러한 정보 자산을 보호하기 위한 체계적인 보안관리가 필수적이다.

신뢰할 수 있는 정보보안 체계를 구축하기 위해서는 다양한 분야의 기술적·관리적 요소를 복합적으로 적용하여야 하는데, 그 핵심에는 데이터를 직접적으로 보호하는 암호기술이 필수적이다. 암호기술은 데이터의 기밀성, 무결성, 인증 및 부인방지와 같은 기본적인 보안 서비스를 제공하여, 모든 정보보안 체계의 기초를 이루는 기반 기술로 인식되고 있다. 따라서 정보시스템 등에 사용되는 암호기술의 안전성과 신뢰성 확보는 그 시스템의 정보보안 수준을 결정짓는 중요한 요소라 할 수 있다.

그러나 암호기술의 안전성은 영구적으로 보장되는 것이 아니다. 암호의 안전성은 공격 기술 발전과 컴퓨팅 성능의 향상에 따라 점차 저하된다. 실제로 과거 안전하다고 평가되었던 암호 알고리즘이나 키 길이가 새로운 분석기법의 개발이나 연산 기술의 발전으로 인해 더 이상 충분한 안전성을 제공하지 못하게 되는 사례가 반복적으로 발생해 왔다. 그 결과 당시에 권고되던 80비트 보안 강도가 112비트로 상향되었으며[56], 연관키 공격[24][26]과 같은 새로운 분석기법의 등장 또한 이러한 기준 상향의 배경이 되었다. 따라서 기술 환경의 변화에 맞추어 지속적이고 주기적으로 암호의 안전성 기준을 검토하고 갱신하여야 한다.

**암호 안전성의 지속적 재검토 필요성을 보여준 사례**

① DES : 56비트의 짧은 키로 인해 1998년 전용 해독 장비가 수십 시간 만에 전수조사로 키 복구에 성공[36], 이후 AES로 대체

② MD5 : 널리 쓰이던 128비트 해시함수로, 2004년 충돌쌍 발견[63] 후 2012년 악성코드 'Flame'이 이를 악용해 위조된 코드서명 인증서를 생성[48]

③ SHA-1 : 160비트 해시함수로 표준화되었으나 2005년 이론적 충돌 공격이 제시되고[62] 2017년 실제 충돌쌍(SHAttered)이 발견되어[59], 전자서명 등 충돌 저항성이 필요한 용도에서 사용 중단

이러한 불가피한 안전성 저하에 더하여, 최근에는 양자컴퓨터의 발전이 암호기술 전반에 대한 새로운 위협으로 인식되고 있다. RSA, ECC 등 인터넷통신 · 전자상거래 등에 널리 사용되는 비대칭 키 암호의 안전성 기반이 되는 수학적 문제는 양자컴퓨터로 구현한 Shor 알고리즘[1]에 의해 빠르게 풀릴 수 있다. 또한 양자컴퓨터에서 동작하는 Grover 알고리즘[2]은 블록암호와 해시함수의 공격 복잡도를 감소시킬 수 있는 것으로 알려져 있기 때문이다. 이에 더해, 암호화된 데이터를 미리 수집해 두었다가 추후 양자컴퓨터 등으로 해독 역량을 확보한 후 복호화를 시도하는 "harvest now, decrypt later" 공격을 함께 고려한다면, 현재의 암호기술로 안전하게 보호되고 있는 정보가 미래에도 여전히 안전할 것이라고 장담할 수 없다. 따라서 장기적으로 보호하여야 하는 국가 · 공공 영역의 중요 정보에 대해서는 한발 앞선 대응이 필요하다.

이 문서는 위와 같은 기술적 배경 및 양자컴퓨터 등 기술 발전 현황을 고려하여, 국가 · 공공 정보시스템에 적용되는 암호기술의 일관성 있는 안전성 기준을 제시하기 위해 작성되었다. 이 문서는 시기별 암호 보안 강도 기준과,

1 Shor 알고리즘 : Peter Shor가 1994년에 제안한 양자 알고리즘이다. 이를 이용하면 정수의 소인수분해와 이산대수 문제를 다항식 시간에 해결할 수 있게 된다[58]. 따라서 충분히 우수한 양자컴퓨터가 개발되면 소인수분해와 이산대수 문제의 어려움에 안전성을 기반하고 있는 RSA · ECC 등 비대칭 키 암호는 쉽게 해독할 수 있게 된다.

2 Grover 알고리즘 : Lov Grover가 1996년에 제안한 양자 알고리즘이다. 정렬되지 않은 N개의 데이터에서 원하는 항목을 약 제곱근($\sqrt{N}$) 수준의 복잡도로 탐색한다[40]. 이를 이용하면 블록암호 키 전수조사나 해시함수 충돌쌍 탐색의 복잡도를 감소시킬 수 있는 것으로 알려져 있다.

그에 대응하는 알고리즘, 키 길이의 사용 정책 그리고 양자컴퓨터 대응 암호체계 전환 추진 방향을 담고 있다. 특히, 종류별 암호 알고리즘의 사용 가능 여부뿐만 아니라 비트(bit) 단위의 계산적 안전성으로 표현되는 보안 강도(security strength)를 기반으로 키 길이 등을 체계적으로 제시하여 국가·공공에 안전한 암호기술을 적용하기 위한 기준을 더 명확히 하고자 노력하였다.

다만, 이 문서에서 언급된 사항은 2026년 현재 시점의 정책 방향으로, 미래 기술의 발전 현황(양자컴퓨터, 암호 분석기술 발전 등)에 따라 변경될 수 있다.

이 문서는 다양한 정보통신 분야 응용 환경에 공통으로 적용할 수 있도록 추상적, 포괄적으로 작성하였다. 이 문서를 근거로 국가·공공 정보시스템 전반에 안전한 암호기술을 도입할 수 있는 정책을 수립하고, 따라서 변화하는 정보보안 환경에 능동적으로 대응할 수 있는 환경을 조성하는 데에 이바지할 수 있기를 기대한다.

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



Chapter 02

# 보안 강도 기준 수립 방침

Chapter 02

# 보안 강도 기준 수립 방침

## 제1절 암호의 보안 강도

### ❶ 기존(classical) 컴퓨터 환경에서 암호의 보안 강도

암호의 보안 강도는 그 암호를 무력화하기가 얼마나 어려운지를 나타내는 척도이다. 기밀성을 위한 블록암호, 공개 키 암호화 등의 보안 강도는 공격자가 키를 알아내거나 평문을 해독하는 데 필요한 최소한의 연산 자원으로, 해시 함수, 전자서명, 메시지 인증코드 등은 키를 알아내거나 메시지를 위조하는 데 필요한 최소한의 연산 자원으로 그 보안 강도를 가늠한다.

암호 알고리즘의 종류에 따라 다르게 측정되는 보안 강도를 일관성 있게 표현하기 위한 단위로 '비트'를 사용한다. 어떤 알고리즘의 보안 강도가 $n$ 비트라는 말은 그 알고리즘을 무력화하는 데에 필요한 최소한의 연산 자원이 대략 $2^n$임을 의미한다. 예를 들어 어떤 암호 알고리즘의 키 길이가 128비트이고, 키 전수조사보다 효과적인 다른 공격이 발견되지 않았다고 가정하자. 그러면, 그 암호 알고리즘을 무력화하는 공격을 반드시 성공시키기 위해서는 최소 $2^{128}$회의 암호 알고리즘 동작이 필요하다. 이런 경우에 그 암호 알고리즘의 보안 강도를 '128비트'라고 표시한다.

대칭 키 암호의 보안 강도는 해당 암호기술의 특성에 따라 키 전수조사 공격의 복잡도나 충돌쌍의 발생 확률 등을 고려하여 산정한다. 블록암호와 같이 비밀 키를 사용하는 경우, 키 전수조사는 $k$ 비트 키가 가질 수 있는 모든 값을 시험하는 방법이다. 이를 위해서는 $2^k$회의 암호 알고리즘 동작이 필요하고 따라서 보안

강도가 $k$비트라고 말한다. 해시함수의 경우 $2^{h/2}$개의 랜덤한 입력에 대하여 $h$비트 해시값을 서로 비교하였을 때 같은 해시값을 출력하는 서로 다른 두 입력, 즉 충돌쌍이 존재할 가능성이 1/2보다 크다. 따라서 해시값의 길이가 $h$비트인 해시함수의 충돌쌍 공격에 대한 보안 강도는 $h/2$비트라고 말한다.

반면, 비대칭 키 암호인 공개 키 암호화와 전자서명의 보안 강도는 대칭 키 암호와는 다른 방식으로 산정한다. 공개 키 암호화와 전자서명은 수학적 난제의 어려움에 안전성을 기반하여 설계되므로, 난제를 해결하면 그 난제에 기반하여 설계한 암호 알고리즘을 무력화할 수 있다. 따라서 주어진 난제를 해결하는 알고리즘의 계산복잡도로 암호 알고리즘의 보안 강도를 산정한다.

정수의 소인수분해 문제에 기반한 RSA의 경우를 살펴보자. RSA를 공격하는 방법의 하나는 공개 키로 사용하는 큰 정수 N을 소인수로 분해하는 것이다. 그리고 소인수분해를 수행하는 데에는 GNFS(general number field sieve) 알고리즘[29]이 가장 효과적인 것으로 알려져 있다. 그런데, GNFS 알고리즘의 계산복잡도를 고려하면, 두 소수의 곱으로 만들어진 공개 키 N의 길이가 1,024비트일 때 약 $2^{80}$번의 단위 연산이, 2,048비트일 때 약 $2^{112}$번의 단위 연산이, 3,072비트일 때 약 $2^{128}$번의 단위 연산이 요구된다. 이런 이유로 공개 키의 크기가 3,072비트인 RSA의 안전성을 128비트라고 말한다.

### ❷ 양자컴퓨터 환경에서 암호의 보안 강도

양자내성암호는 기존 컴퓨터는 물론이고, 양자컴퓨터로도 다항식 시간[3]에 해결하는 알고리즘이 알려지지 않은 새로운 수학적 난제에 기반하거나, 또는 대칭 키 암호의 안전성에 기반하여 설계한다. 구체적으로는 격자 상의 LWE 또는 SVP 문제, 오류정정부호의 신드롬 디코딩 문제, 다변수 다항식의 해 탐색 문제에 기반하거나 해시함수의 역상 안전성에 기반하여 양자내성암호를 설계

3 다항식 시간 알고리즘은 풀고자 하는 문제의 규모가 커질수록 알고리즘 수행 시간이 증가하는 비율이 문제 크기의 다항식 수준이라는 의미다. 일반적으로 문제의 규모가 커져도 시간이 많이 늘어나지 않아 빠르게 동작하는 알고리즘이며, 따라서 문제를 해결할 수 있는 다항식 시간 알고리즘이 알려진 경우 쉬운 문제로 인식된다.

한다. 이러한 양자내성암호의 기반 문제를 해결하는 고전적인 알고리즘은 지수 또는 준지수 시간[4] 알고리즘만 알려진 상태이다. 그리고 양자컴퓨터를 사용한다고 하더라도 기존 알고리즘의 일부 과정을 Grover 알고리즘으로 가속하는 수준이다.

국제 표준기구인 ISO/IEC는 기존 컴퓨터와 양자컴퓨터가 공존하는 상황에서도 암호 알고리즘의 안전성을 일관되게 가늠할 수 있도록 [표 1]과 같이 안전성 범주를 정하였다. 이 범주는 블록암호와 해시함수의 해독에 필요한 기존 컴퓨터와 양자컴퓨터의 연산량을 기준으로 나누었다.

예를 들어 어떤 양자내성암호 알고리즘이 안전성 범주 C1에 포함된다는 것은 이 알고리즘을 기존 컴퓨터 또는 양자컴퓨터로 무력화하기 위해 적어도 키 길이가 128비트인 블록암호(예 : AES-128)의 키 탐색을 각각의 컴퓨터로 수행하는 수준의 공격량이 필요하다는 의미이다. 같은 방법으로 안전성 범주 C3, C5는 각각 키 길이가 192, 256비트인 블록암호의 키 탐색 공격을 기준으로 정의하였다. 그리고 C2, C4는 각각 출력 길이가 256, 384비트인 해시함수(예 : SHA3)의 충돌쌍 탐색 공격을 기준으로 정의하였다.

이 문서는 양자내성암호의 안전성을 표시하기 위해 ISO/IEC가 [표 1]과 같이 정의한 안전성 범주를 준용하였다.

**[표 1] 양자컴퓨터를 고려한 국제 표준기구(ISO/IEC)의 암호 안전성 기준**

| 안전성 범주 | 공격 유형 및 기준 | 대상 알고리즘(예) |
|---|---|---|
| C1 | 128비트 키 블록암호의 키 탐색에 안전 | AES-128 |
| C2 | 256비트 해시함수의 충돌쌍 탐색에 안전 | SHA3-256 |
| C3 | 192비트 키 블록암호의 키 탐색에 안전 | AES-192 |
| C4 | 384비트 해시함수의 충돌쌍 탐색에 안전 | SHA3-384 |
| C5 | 256비트 키 블록암호의 키 탐색에 안전 | AES-256 |

4 지수/준지수 시간 알고리즘은 문제의 규모에 비해 해결에 걸리는 시간이 (준)지수적(기하급수적)으로 증가하는 알고리즘인데, 해결하는 방법으로 지수/준지수 시간 알고리즘밖에 알려지지 않은 문제는 어려운 문제로 인식된다.

### 양자컴퓨터를 이용한 암호공격

양자컴퓨터는 양자역학의 중첩(superposition)과 얽힘(entanglement) 현상을 이용하여 연산을 수행하는 장치를 말한다. 이러한 양자컴퓨터를 이용하면, 어떤 작업을 할 때 필요한 동작 시간을 기존 컴퓨터에 비해 현저히 줄이거나, 기존 컴퓨터로는 해결하기 어렵다고 여기던 어떤 문제를 쉽게 풀 수 있게 된다. 그 대표적인 예가 Grover 알고리즘과 Shor 알고리즘이다.

#### ① Grover 알고리즘

Grover 알고리즘은 정렬되지 않은 다량의 데이터 중 조건을 만족하는 데이터를 빠르게(전체 데이터 개수의 제곱근 정도의 연산) 찾는 양자 알고리즘이다. 이 알고리즘은 주로 대칭 키 암호를 공격하는 데 사용된다. 이론적으로는 블록암호 키 전수조사의 복잡도를 기존의 제곱근 수준으로 낮추고, 해시함수의 충돌쌍 탐색의 복잡도를 기존 복잡도의 2/3 제곱 수준으로 낮출 수 있다[27]. 따라서 이론이 그대로 실현된다면 이에 대응하기 위하여 키 길이가 더 긴 블록암호를 사용하거나, 출력 길이가 더 긴 해시함수를 사용해야 한다.

그러나 Grover 알고리즘에 기반한 암호공격은 현실적으로 한계가 있다. 먼저, 양자컴퓨터를 사용한 키 탐색 과정과 기존 컴퓨터를 사용한 키 전수조사를 같은 선상에서 비교하기에는 컴퓨팅 환경의 차이에서 발생하는 기본 단위 연산의 차이가 크다. 그리고, Grover 알고리즘은 병렬화로 인한 고속화 비율의 제곱에 비례하는 개수의 장치가 필요하다. 예를 들어 양자컴퓨터 1대당 연산시간을 1/10로 줄이고자 하면, 100대의 양자컴퓨터가 필요하다.

알고리즘의 고속화와 별개로, 현재 기술로는 아직 fault-tolerant 양자컴퓨터[5]를 만들 수 없으므로 양자컴퓨터 연산 수행 시간에는 제약이 있고, 따라서 병렬화가 필수적이다. 만약 미래에 fault-tolerant 양자컴퓨터가 만들어지더라도 공격을 수행하는 양자컴퓨팅 회로의 크기(큐비트의 수)에는 한계가 존재한다. 따라서 실제 공격을 위한 회로의 최대 크기(MAXDEPTH)를 고려한 병렬화 수준의 결정이 필요하게 된다.

결과적으로 Grover 알고리즘 기반 암호공격에는 상당한 수준의 양자컴퓨터 병렬화가 필수적이다. 그리고 병렬화 과정에서 요구되는 물리적 자원과 계산복잡도의 증가 등을 고려하면 실제 공격에 필요한 자원은 알고리즘이 보장하는 제곱근 가속에 따른 공격량 절감 효과를 온전히 누리지 못한다. 그러므로 대칭 키 암호의 보안 강도는 양자컴퓨터를 사용한 공격으로 인해 현저하게 저하되지는 않을 것으로 판단한다.

---

5 Fault-tolerant 양자컴퓨터는 연산 과정에서 발생하는 오류로 인한 큐비트의 상태 붕괴 없이 지속적인 연산이 가능한 양자컴퓨터를 의미한다.

② Shor 알고리즘

반면, 양자컴퓨터에 대한 비대칭 키 암호의 보안 강도는 전혀 다른 양상을 가진다. Shor 알고리즘은 어떤 함수의 주기(period)를 찾는 다항식 시간 양자 알고리즘이다. 그리고 이를 이용하면 정수의 소인수분해나 이산대수 문제를 쉽게 해결할 수 있다. 따라서 양자컴퓨터를 이용하면 이런 문제의 어려움에 기반하여 만들어진 비대칭 키 암호 알고리즘을 쉽게 무력화 할 수 있다. 그러므로 충분한 개수의 큐비트를 효율적으로 사용하는 양자컴퓨터가 만들어지면, RSA, ECC 등 지금까지 주로 사용해 온 비대칭 키 암호는 키 길이 등 안전성 파라미터의 크기에 상관없이 더 이상 안전하지 않게 된다.

Shor 알고리즘으로 RSA-2048을 해독하는 데 필요한 양자컴퓨터의 규모(자원)는 양자컴퓨터 관련 연구의 진전에 따라 지속적으로 낮아지고 있다. 큐비트의 개수로만 보았을 때, 2021년에는 약 2천만 큐비트가 필요한 것으로 추정되었으나[38] 2025년에는 100만 큐비트 미만으로 낮추는 분석이 제시되었다[37]. 하드웨어 측면에서도 2024년 구글이 큐비트 수를 늘릴수록 오류율이 낮아지는 오류정정 성과를 보고하는 등[39] 관련 연구가 빠르게 진전되고 있다.

## 제2절 보안 강도 기준 수립 고려 사항

이 문서에서 제시하는 국가·공공 암호 보안 강도 기준 및 알고리즘 사용 정책을 수립하기 위하여 다음 사항을 고려하였다.

- 국내외 암호 사용 관련 정책 및 제도 연계성
- 보안 강도 상향과 양자내성암호로의 안정적 전환
- 양자컴퓨터 기반 암호공격의 실현 가능성

### ❶ 국내외 암호 사용 관련 정책 및 제도 연계성

우선 우리나라를 포함하여 주요국의 암호 사용 관련 정책 및 제도의 근거가 되는 암호 안전성 기준 관련 문서를 정리하면 [표 2]와 같다.

그리고 국내 개발 암호 알고리즘의 사용 정책 제시를 위하여 검증필 암호모듈 현황 등 산업계의 암호 알고리즘 사용 현황을 참고하였다. 국가·공공 분야에

적용할 암호에 대한 기준이므로, 국내 암호모듈 검증제도(이하 KCMVP)의 검증대상 암호알고리즘을 안전성 파라미터 기준 수립의 주요 대상으로 하였다.

암호 알고리즘 사용 기준 수립에 있어 주요 쟁점 중 하나는 양자내성암호의 적용이다. 정부는 관계부처 합동으로, 2035년까지 양자내성암호로 전환하는 것을 목표로 『범국가 양자내성암호 전환 마스터플랜』과 세부 계획인 『범국가 양자내성 암호체계 전환 종합 추진계획』을 2023년과 2025년에 각각 발표하였다 [1][2]. 이 문서는 마스터플랜과 해당 종합 추진계획에서 제시한 전환 로드맵을 반영하여 암호의 종류와 보안 강도에 따른 사용 정책 변경 시기를 설정하였다. 다만, 양자내성암호는 아직 KCMVP 검증대상으로 지정된 알고리즘이 없는 상태이다. 따라서 2026년 현재 국제 표준이거나, 표준화가 진행 또는 논의 중인 여러 양자내성암호 알고리즘을 사용 기준 수립의 주요 대상으로 설정하였다.

**[표 2] 국내외 암호 안전성 기준 관련 문서**

| 국가 | 기관 | 문서 |
|---|---|---|
| 대한민국 | NIS | • 국가·공공기관 암호 사용 기준 |
| | NIS, NSR | • 암호모듈 구현안내서 Part 1 : 시험 및 구현 사례별 해설서<br>• 암호모듈 구현안내서 Part 2 : 검증대상 암호알고리즘 구현안내서 |
| | KISA | • 암호 알고리즘 및 키 길이 이용 안내서 |
| 미국 | NIST | • NIST Special Publication 800-57 Recommendation for Key Management |
| | | • NIST Special Publication 800-131A Revision 3 (ipd) Transitioning the Use of Cryptographic Algorithms and Key Lengths |
| | | • NIST IR 8547 Transition to Post-Quantum Cryptography Standards |
| 캐나다 | CCCS | • ITSP.40.111 Cryptographic algorithms for UNCLASSIFIED, PROTECTED A and PROTECTED B information |
| | | • ITSM.40.001 Roadmap for the migration to post-quantum cryptography for the Government of Canada |
| 유럽연합 | ECCG | • Agreed Cryptographic Mechanisms |

| 국가 | 기관 | 문서 |
|---|---|---|
| 독일 | BSI | • BSI TR-02102-1 Cryptographic Mechanisms : Recommendations and Key Lengths |
| 프랑스 | ANSSI | • ANSSI-PG-083 Règles et recommandations concernant le choix et le dimensionnement des mècanismes cryptographiques |
| 네덜란드 | ICBR | • Rijksbreed beleidskader cryptografie : Een raamwerk voor het opstellen van cryptografiebeleid |
| | NCSC-NL | • Transport Layer Security (TLS) Security guidelines |
| | AIVD, CWI, TNO | • The PQC Migration Handbook |
| 영국 | NCSC-UK | • Using TLS to protect data |
| | | • Timelines for migration to post-quantum cryptography |
| 일본 | CRYPTREC | • CRYPTREC LS-0001-2022R2 List of Ciphers to be Referred to in Procurement for e-Government |
| | | • CRYPTREC LS-0003-2022r1, Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection) |

2026년 기준 해외 주요국과 국내의 암호 관련 정책 동향을 정리하기 위하여 [표 2]의 문서들을 분석한 내용을 부록으로 수록하였다.

## ❷ 보안 강도 상향과 양자내성암호로의 안정적 전환

국가·공공 영역의 암호 알고리즘 사용기준은 국가정보원이 2009년 발간, 국가·공공기관에 배포한 『국가·공공기관 암호 사용 기준』[3]에서 제시하고 있다. 이 기준은 배포 당시 비밀 등 비공개 정책이 포함되어 있어 국가·공공기관 대상으로만 대외비로 배포되었다.

이 암호 사용 기준은 국가·공공기관 업무환경에 맞는 최적의 암호기술 도입·사용 등 비밀 또는 행정정보 보호를 위해 준수해야 할 정책·기술적 기준을 제시하고 행정기관 표준 암호 알고리즘 목록과 함께 정보의 보안등급별 암호사용 기준을 명시하고 있다.

민간 영역의 암호 알고리즘 사용 기준은 과학기술정보통신부와 한국인터넷진흥원(KISA)이 발간한 『암호 알고리즘 및 키 길이 이용 안내서』[6]를 통하여 보안 강도가 112비트인 암호의 사용을 2030년까지 허용하고 있으며, 2031년 1월부터는 암호의 보안 강도를 128비트로 상향하도록 안내하고 있다.

한편, 앞서 언급한 국내 양자내성암호 전환 정책에 따르면 양자내성암호로 전면 전환되는 시기를 2036년으로 정하고 있어 경우에 따라 2035년까지 기존 비대칭 키 암호를 사용하는 경우가 발생할 수 있다. 따라서 2026년 현재 보안 강도가 112비트인 암호를 사용 중인 시스템을 2035년에 양자내성암호로 전환하기 위해서는 2031년 이전에 보안 강도가 128비트인 기존 비대칭 키 암호로 전환한 후 다시 양자내성암호로 전환하거나 양자내성암호로 바로 전환하는 것을 고려하여야 한다.

이 문서에서는 2031년부터 양자내성암호로 전면 전환되는 2036년까지의 기간을 위하여 막대한 사회적 비용이 예상되는 기존 비대칭 키 암호의 보안 강도 상향을 유도하는 것이 불가피한 선택인지 고려하였다.

우선, 양자컴퓨터 위협을 제외하고 GNFS 알고리즘 등의 발전 양상을 고려할 때, 가까운 미래에 보안 강도가 112비트인 기존 비대칭 키 암호의 사용을 금지해야 할 만큼 위협적인 수준으로의 발전은 예상되지 않는다. 또한 국내에서는 암호모듈 검증제도의 운영 정책을 고려할 필요가 있는데, 2026년 현재 KCMVP는 보안 강도가 112비트인 해시함수, 공개 키 암호화, 전자서명, 키 설정의 사용을 허용하고 있으며, 신규로 검증을 신청하는 모듈은 128비트 이상의 보안 강도를 가지는 알고리즘을 의무 탑재하도록 하여 보안 강도의 상향을 이미 자연스럽게 유도하고 있다.

이런 이유로 2031년부터는 암호의 보안 강도를 128비트 이상으로 상향하도록 안내해 온 기존의 국내 정책과는 다르게, 양자내성암호로 전면 전환되는 2036년 이전까지 보안 강도가 112비트인 기존 비대칭 키 암호의 사용을 한시적으로 허용하여 불필요한 사회적 비용을 줄이는 방향으로 기준을 수립하였다.

또한 양자내성암호로의 안정적 전환을 위하여 일정 기간 기존 비대칭 키 암호와 함께 사용하는 방향을 고려하였다.

양자컴퓨터의 위협은 최근 수년간 실현 가능성이 점점 커지고, 그 시기도 점점 앞당겨지는 추세이다. 그리고 그로 인하여 개발 후 충분한 검증 기간을 가지지 못한 양자내성암호 알고리즘의 표준화가 논의되거나, 양자내성암호의 안전성 분석기술의 발달에 따른 새로운 취약점 도출 사례가 발생하기도 하였다. 2022년에 발표된 SIDH, SIKE 알고리즘[6]의 공격[30]과 40년 이상 안전성을 유지해 온 오류정정부호 기반 Classic McEliece 알고리즘의 새로운 분석 기법[41]의 발표가 그 좋은 예이다. 이를 보완하기 위한 방법으로, 한 가지 기능을 위해 여러 암호 알고리즘을 동시에 적용하는 하이브리드 방식을 고려할 수 있다. 암호모듈 검증제도는 2025년 7월부터 이미 양자내성암호와 기존 비대칭 키 암호의 하이브리드 방식에 대한 검증을 시행하고 있고, 2025년 12월에 개정된 『암호모듈 구현안내서 Part 1』[4]도 양자내성암호를 포함하는 하이브리드 방식의 암호모듈 구현 방식을 안내하고 있다.

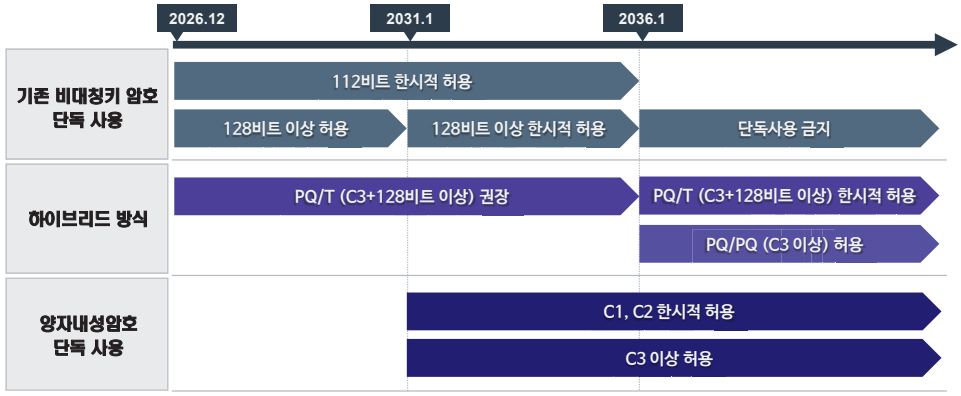
이러한 점을 고려하여 양자내성암호로의 완전한 전환에 앞선 기간에는 기존 비대칭 키 암호와 양자내성암호를 함께 적용하는 하이브리드 방식을 사용하고, 양자내성암호로 전환을 완료한 2036년부터는 기반 문제가 서로 다른 여러 양자내성암호의 하이브리드 방식을 권장하는 방향으로 기준을 수립하였다.

결과적으로 이 문서에서는 2036년 이전에는 보안 강도가 112비트인 기존 비대칭 키 암호를 한시적으로 사용할 수 있도록 하였다. 또, 2035년까지는 기존 비대칭 키 암호와 양자내성암호의 하이브리드(PQ/T, Post-quantum/Traditional)를 권장하고, 2036년부터는 양자내성암호끼리의 하이브리드(PQ/PQ, Post-quantum/Post-quantum)를 권장하는 방향으로 기준을 수립하였다.

이 문서에서 수립한 보안 강도 기준의 적용 시점을 시간순으로 정리하면 [그림 1]과 같다.

6 SIDH, SIKE 알고리즘은 오랫동안 양자내성 난제로 인식 되어온 타원곡선 사이의 아이소제니 문제에 기반한 알고리즘이다. 위 공격으로 인하여 아이소제니 기반 암호가 모두 해독된 것은 아니었지만, 이후 관련 연구에 대한 관심이 많이 줄어들었다.

**[그림 1] 국내 비대칭 키 암호 사용 전환 로드맵**




## 비대칭 키 암호의 사용 방식

비대칭 키 암호의 사용 방식은 크게 단독 사용 방식과 하이브리드 사용 방식으로 구분할 수 있다.

### ① 단독 사용

비대칭 키 암호 알고리즘 하나만 사용하여 데이터 암호화나 전자서명, 키 설정 등을 수행하는 것을 말한다. 지금까지 암호를 사용하는 대부분의 방식이 단독 사용이었다. 그러나 양자내성 암호 전환을 앞두고, 미래에 다가올 공격에 대한 대비와 암호 민첩성(crypto agility) 등을 고려할 때, 비대칭 키 암호의 단독 사용 안전성에 대한 검토가 필요한 상황이다.

### ② 하이브리드 사용

이 문서에서 하이브리드[7]는 같은 기능을 하는 둘 이상의 비대칭 키 암호 알고리즘을 함께 사용하여 정보를 보호하는 방식을 의미한다. 하이브리드 방식은 함께 사용하는 알고리즘 중 일부가 취약해지더라도 전체 기능의 안전성이 저하되지 않도록 하기 위하여 사용한다. 그러므로 보안 강도가 대등한 알고리즘의 결합을 원칙으로 하며, 하나의 알고리즘을 공격하여 얻은 정보로 다른 알고리즘을 쉽게 무력화할 수 없도록 설계하여야 한다.

---

7 암호 분야에서는 오랫동안 공개 키 암호 기술로 비밀 키를 공유하고 그 키로 대칭 키 암호 통신을 수행하는 KEM-DEM 암호화 방식을 '하이브리드 암호체계(hybrid cryptosystem)'라고 표현해 왔다. 그러나 이 문서의 '하이브리드'는 이것을 의미하지는 않는다.

하이브리드는 결합하는 알고리즘의 종류에 따라, 기존 비대칭 키 암호와 양자내성암호를 결합하는 PQ/T 하이브리드와 양자내성암호끼리 결합하는 PQ/PQ 하이브리드로 구분할 수 있다.

PQ/T 하이브리드[8]는 기존 비대칭 키 암호에 대한 양자컴퓨터 기반 암호해독 위협과 양자내성암호의 암호학적 성숙도 부족을 동시에 보완하기 위한 하나의 방법으로 논의되고 있다. "harvest now, decrypt later" 공격에 대응하기 위해 양자내성암호의 우선 적용이 필요하지만, 아직 발견되지 않은 결함이 드러날 가능성을 고려하여 기존 비대칭 키 암호 성분이 안전성을 유지하도록 한다. 향후 양자컴퓨터가 충분히 발전하면 기존 비대칭 키 암호 성분은 안전성을 유지하기 어려우므로 양자내성암호 성분이 안전성을 보장한다.

PQ/PQ 하이브리드는 특정 난제에 대한 해독 기술이 발전하더라도 안전성이 유지되도록 서로 다른 수학적 난제에 기반한 양자내성암호를 결합하는 방식이다. 예를 들면 격자와 오류정정부호처럼 기반 문제가 서로 다른 알고리즘을 결합할 때 그 목적을 달성할 수 있으며, 기반 문제가 같은 알고리즘끼리 결합할 때에는 이러한 효과를 기대하기 어렵다.

하이브리드 방식은 키 설정과 전자서명으로 구분하여 기술개발 및 IETF 중심의 표준화가 논의 중이다. 특히 하이브리드 전자서명은 알고리즘의 결합 방식과 동시에 인증서 규격의 표준화도 함께 논의되고 있다.

## ❸ 양자컴퓨터 기반 암호공격의 실현 가능성

양자컴퓨터의 성능이 기존 공개 키 암호체계를 실질적으로 위협할 수준에 도달하는 시점에 대해서는 다양한 전망이 존재하지만, 국내외 정부와 연구기관은 2030년대 초반에서 후반(2030~2040년경)을 잠재적 위험 시점으로 예측하고 있다. 실제로 Global Risk Institute가 매년 발간하는 Quantum Threat Timeline Report[50]에 따르면, 국제 전문가들은 암호학적으로 유의미한 양자컴퓨터(cryptographically relevant quantum computer, CRQC)가 향후 10년 이내에 등장할 확률을 약 28~49%, 15년 이내에 등장할 확률을 약

8 PQ/T 하이브리드는 하이브리드-AND와 하이브리드-OR로 구분하여 논의하기도 한다. 하이브리드-OR 방식은 공격자가 기존 비대칭 키 암호 또는 양자내성암호 중 한 가지를 공격할 수 있으면 전체가 위협을 받는 방식을 의미한다. 이 문서는 암호 알고리즘 자체의 안전성을 다루므로, 하이브리드-OR 방식은 '단독 사용'과 같은 것으로 간주하여 별도로 고려하지 않는다.

51~70%로 예측하였다. 그리고 “harvest now, decrypt later” 공격과 Mosca의 부등식[49]을 고려한다면, 보호 대상 정보의 기밀 유지 요구 기간과 암호체계 전환에 필요한 기간을 합한 값이 CRQC 등장까지 남은 기간보다 길어서는 안 되므로, 그에 대한 대비는 실질적인 위협이 닥쳐올 시점보다 상당히 앞서 완료해야 한다.

Grover 알고리즘을 이용한 대칭 키 암호공격은 대규모 장비(큐비트)가 필요하지는 않으나 회로의 깊이가 깊다는 단점이 있다. 그리고 병렬화를 위해 회로의 깊이를 줄이면, 줄어든 비율의 제곱에 비례하는 규모의 장비(큐비트)가 필요하다. 이런 이유로 공격 자체의 현실성이 떨어진다고 판단하였다. 따라서 대칭 키 암호에 대해서는 양자컴퓨터 기반 암호공격을 이유로 키 길이 등 파라미터를 상향하는 방향으로 기준을 수립하지는 않았다. 그러나 여러 가지 잠재적 가능성을 고려하여 높은 안전성을 제공하는 파라미터의 사용을 권장하였다.

그에 비하여 Shor 알고리즘을 이용한 비대칭 키 암호공격은 다소 많은 큐비트가 필요하지만 다항식 시간 알고리즘으로 인해 효율적임을 고려하였다. 그리고 양자컴퓨팅 기술의 발전으로 충분한 큐비트가 확보될 가능성이 점점 높아질 것으로 예상됨에 따라 현실적인 위협으로 작용한다고 판단하였다. 따라서 기존의 비대칭 키 암호는 적절한 시점에 사용을 금지하고, 양자내성암호와 하이브리드 방식을 사용하여 전환을 유도하도록 하였다.

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



Chapter 03

# 암호 알고리즘 사용 기준

Chapter 03

# 암호 알고리즘 사용 기준

이 문서에서는 암호의 종류에 따른 보안 강도 기준과 시기별 사용 정책을 제시하고 있다. 또 알고리즘별로 세부 기준 및 그 기준을 충족시키기 위해 요구되는 안전성 파라미터의 구체적인 값을 제시하고 있다. 이와 관련하여, 암호 알고리즘의 사용에 관한 표현과 용어의 정의는 [표 3], [표 4]와 같다.

**[표 3] 암호 알고리즘 사용 형태에 관한 표현**

| 표현 | 정의 |
|---|---|
| 암호학적 보호 | 데이터를 보호할 목적으로 암호 알고리즘의 기능(암호화, 해시, 인증값 생성, 전자서명 등)을 사용함 |
| 암호학적 처리 | 보호된 데이터를 확인할 목적으로 암호 알고리즘의 기능(복호화, 해시, 인증값 검증, 전자서명 검증 등)을 사용함 |

**[표 4] 암호 알고리즘 시기별 사용 정책에 관한 표현**

| 용어 | 정의 | 비고 |
|---|---|---|
| 허용 | 정보의 보호와 처리에 모두 사용할 수 있음 | 사용 가능 (암호학적 보호와 처리에 모두 사용할 수 있음) |
| 한시적 허용 | 향후 사용을 제한 또는 금지할 예정으로, 사용 중인 암호 알고리즘의 교체 시점과 방식을 검토하여야 함 | |
| 제한 | 보호된 데이터의 처리에만 암호 알고리즘을 사용할 수 있고, 새로운 데이터의 보호에는 사용할 수 없음 | 사용 가능 (암호학적 처리에만 사용할 수 있음) |
| 금지 | 암호 알고리즘을 보호와 처리에 사용할 수 없음 | 사용 불가 |

## 제1절 국가·공공 암호 알고리즘 사용 기준 총괄

국가·공공 분야 정보시스템 등에 적용하는 암호의 보안 강도 기준과 사용 정책을 총괄하면 [표 5]와 같다. 암호기술을 대칭 키 암호와 비대칭 키 암호로 구분하고, 시기별로 보안 강도 수준에 따른 사용 기준을 명시하였다. 또 양자내성암호 전환을 고려하여 양자내성암호와 하이브리드 방식의 적용 정책도 명시하였다.

**[표 5] 암호 알고리즘 사용 기준 총괄**

<table>
<tr><th colspan="3">암호 구분</th><th colspan="2">보안 강도</th><th>2030년<br>12월까지</th><th>2031년<br>1월부터</th><th>2036년<br>1월부터</th></tr>
<tr><td colspan="3" rowspan="4">대칭 키 암호</td><td colspan="2">112비트</td><td>한시적 허용</td><td colspan="2">제한</td></tr>
<tr><td colspan="2">128비트</td><td>허용◈</td><td colspan="2">허용</td></tr>
<tr><td colspan="2">192비트</td><td colspan="3">허용◈</td></tr>
<tr><td colspan="2">256비트 이상</td><td colspan="3">허용◈</td></tr>
<tr><td rowspan="6">비대칭키 암호</td><td rowspan="3">단독사용</td><td>기존 암호</td><td colspan="2">112비트 이상</td><td>허용</td><td>한시적 허용</td><td>금지*</td></tr>
<tr><td>양자내성 암호</td><td colspan="2">C1, C2</td><td>※</td><td colspan="2">한시적 허용</td></tr>
<tr><td>양자내성 암호</td><td colspan="2">C3, C4, C5</td><td>※</td><td colspan="2">허용</td></tr>
<tr><td rowspan="3">하이브리드</td><td rowspan="2">PQ/T</td><td>C1, C2</td><td>112비트 이상</td><td>허용</td><td colspan="2">한시적 허용</td></tr>
<tr><td rowspan="2">C3, C4, C5</td><td>112비트</td><td colspan="2">허용</td><td>한시적 허용</td></tr>
<tr><td>PQ/PQ</td><td>128비트 이상</td><td colspan="2">허용◈</td><td>한시적 허용</td></tr>
<tr><td colspan="2">PQ/PQ</td><td colspan="2">C1, C2</td><td>※</td><td colspan="2">한시적 허용</td></tr>
<tr><td colspan="2">PQ/PQ</td><td colspan="2">C3, C4, C5</td><td>※</td><td colspan="2">허용</td></tr>
</table>

※ : 현재는 별도의 정책을 제시하지 않음, 다만, 알고리즘 구현 측면에서의 충분한 안전성 검증 등 양자내성암호 기술의 성숙도를 고려, 가능한 경우 다른 선택지의 사용을 우선 권장함

◈ : 정보의 장기적 보호를 위해 연산 자원이나 통신환경 등의 제약이 없는 한 우선 적용을 고려할 것을 권장함

∗ : 사용 제한 단계 없이 사용을 금지함

PQ/T, PQ/PQ : 하이브리드 결합 알고리즘에 따른 구분을 의미. 2장 2절 ❷ 참고

C1, C2, C3, C4, C5 : 양자내성암호 안전성 범주를 의미. 2장 1절 ❷의 [표 1] 참고

## 제2절 암호 보안 강도 기준 수립 원칙

- 대칭 키 암호
  - 대칭 키 암호는 블록암호와 이를 기반으로 하는 운영모드, 해시함수, 메시지 인증코드, 난수발생기, 키 유도 함수를 포함한다. 스트림암호는 KCMVP 검증 대상에 포함되지 않았다는 점과 실제 활용도가 높지 않다는 점을 고려하여 이 문서에서 다루지 않는다.
  - 보안 강도가 112비트인 대칭 키 암호는 해시함수와 해시함수에 기반한 알고리즘만 해당한다.
  - Grover 알고리즘을 이용한 양자컴퓨터 기반 암호공격을 보안 강도가 128비트인 대칭 키 암호에 대한 직접적인 위협으로 판단하지는 않았다. 그러나 2031년부터는 구현 환경과 성능에 특별한 제약이 없는 경우에는 보안 강도가 192비트 이상인 대칭 키 암호의 사용을 권장한다.
- 비대칭 키 암호
  - 비대칭 키 암호는 공개 키 암호화와 전자서명 그리고 키 설정(키 합의, 키 캡슐화 메커니즘)을 포함한다.
  - 2036년 1월부터 비대칭 키 암호를 사용한 정보의 보호는 양자내성암호 단독 또는 하이브리드 방식으로 전환한다.
- 기존 비대칭 키 암호 단독 사용
  - 양자내성암호 도입 및 적용이 이미 예정되어 진행되고 있는 경우를 고려, 보안 강도가 112비트인 알고리즘의 사용을 2035년까지 한시적 허용한다.
  - 또한 양자내성암호와의 하이브리드 사용이 활성화되도록 2031년부터는 보안 강도가 128비트 이상인 알고리즘의 사용도 한시적 허용한다.

- 다만, 향후 128비트 보안 강도를 가진 하이브리드 방식 사용 권장 등을 고려, 112비트 보안 강도를 128비트로 한차례 상향 후 양자내성암호로 전환하는 단계적 방식을 우선 권장한다.

- 2036년 1월부터는 사용 제한 단계 없이 모든 알고리즘의 사용을 금지한다. 이는 향후 양자내성암호 관련 정책에 따라 조정될 수 있다.

● 양자내성암호 단독 사용

- 양자내성암호는 2031년 1월부터 단독 사용을 허용하되, 기술의 성숙도를 고려, PQ/T 하이브리드 방식의 사용을 강력히 권장한다.

● 비대칭 키 암호 하이브리드

- PQ/T 하이브리드 방식의 보안 강도는 2036년 1월을 기준으로, 그 이전에는 기존 비대칭 키 암호의 보안 강도로, 그 이후에는 양자내성암호의 보안 강도로 정의한다.

- 2035년까지는 양자내성암호와 기존 비대칭 키 암호와의 하이브리드(PQ/T) 방식으로 사용하는 것을 권장한다.

- PQ/T 하이브리드 방식은 보안 강도가 대등한 알고리즘의 결합을 원칙으로 한다. 다만, TLS 1.3 등 별도로 정해진 규격을 사용하는 경우는 예외로 정할 수 있다.

- PQ/PQ 하이브리드 방식은 안전성 범주가 대등하고, 서로 다른 수학적 난제에 기반한 양자내성암호 2종 이상의 알고리즘 결합을 원칙으로 한다.

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



Chapter 04

# 암호 알고리즘별 사용 정책

Chapter
# 04 암호 알고리즘별 사용 정책

이 장은 제3장에서 정의한 안전성 기준에 따른 암호 사용 정책을 알고리즘별로 정리한다. 알고리즘별로 보안 강도와 이를 제공하기 위한 안전성 파라미터를 안내하고, 그에 따른 시기별 사용 정책을 세부적으로 제시하였다.

이 장에서 주로 다루는 알고리즘은 KCMVP 검증대상 암호알고리즘이다. KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 하며[9] 이때는 [표 5]에 명시된 암호 보안 강도 및 사용 정책을 따라야 한다. 또한 해당 암호 알고리즘의 보안 강도를 가늠하고자 하는 경우, 유사한 파라미터의 KCMVP 검증대상 암호알고리즘별 보안 강도를 참고하기를 권고한다.

이 장에서 다루는 암호기술의 분류별 정의와 간략한 설명, 개념도 및 참조 표준 등을 정리하여 부록으로 수록하였으니 참고하기를 바란다.

## 제1절 대칭 키 암호

### ❶ 블록암호와 블록암호 운영모드

블록암호 알고리즘의 보안 강도와 사용 정책은 [표 6]과 같다.

9 국내 표준은 KS, 국제 표준은 ISO/IEC를 준용하기를 권고하며, 부득이하게 불가한 경우 이와 유사한 수준의 표준화 기구가 표준화한 암호 알고리즘을 사용하기를 권고한다.

**[표 6] 블록암호 알고리즘 보안 강도 기준**

| 알고리즘 | 보안 강도 | 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|
| HIGHT | 128비트 | 128비트 | 한시적 허용 | 제한 | 금지 |
| SEED, LEA-128, ARIA-128, AES-128 | 128비트 | 128비트 | 허용◈ | 허용 | |
| LEA-192, ARIA-192, AES-192 | 192비트 | 192비트 | 허용◈ | | |
| LEA-256, ARIA-256, AES-256 | 256비트 | 256비트 | 허용◈ | | |

- 양자컴퓨터 공격 등을 고려하여 2031년부터는 보안 강도가 192 또는 256비트인 블록암호 알고리즘의 사용을 권장한다. 그러나 이러한 사실이 보안 강도가 128비트인 블록암호 알고리즘의 안전성이 양자컴퓨터 공격으로 저하될 것을 예상한다는 의미는 아니다.

- HIGHT 알고리즘은 다음과 같은 이유로 사용을 금지할 예정이다.

  - 블록 길이가 64비트이므로 인증암호화 모드인 CCM과 GCM에 사용할 수 없음

  - KCMVP 검증필 모듈에 탑재되는 경우가 매우 적고, 호환성 등의 문제로 활용도가 낮음

  - 128비트 키만 사용하므로, 향후 더 높은 보안 강도가 요구되는 환경 등 활용성 확장에 제한이 있음

- KCMVP 검증대상이 아닌 기술에 관한 사항은 다음과 같다.

  - TDEA 알고리즘의 사용을 제한한다. TDEA는 ISO/IEC 18033-3에 명시된 블록암호이며, 2025년 검토에서 제외되지 않아 현재 유효한 국제 표준이다. 그러나 미국은 TDEA를 정의한 NIST SP 800-67을 2024년에 철회하였고, 레거시 환경을 위해 암호학적 처리에만 사용하도록 제한하였다.

– KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.

블록암호 운영모드의 보안 강도와 사용 정책은 [표 7]과 같다.

**[표 7] 블록암호 운영모드 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 블록암호 | 블록암호 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|
| 기밀성 모드 (CBC, CFB, OFB, CTR) | 128비트 | HIGHT | 128비트 | 한시적 허용 | 제한 | 금지 |
| | 128비트 | SEED, LEA–128, ARIA–128, AES–128 | 128비트 | 허용◈ | 허용 | |
| | 192비트 | LEA–192, ARIA–192, AES–192 | 192비트 | 허용◈ | | |
| | 256비트 | LEA–256, ARIA–256, AES–256 | 256비트 | 허용◈ | | |
| 인증 암호화 모드 (CCM, GCM) | 128비트 | SEED, LEA–128, ARIA–128, AES–128 | 128비트 | 허용◈ | 허용 | |
| | 192비트 | LEA–192, ARIA–192, AES–192 | 192비트 | 허용◈ | | |
| | 256비트 | LEA–256, ARIA–256, AES–256 | 256비트 | 허용◈ | | |

- 블록암호 운영모드의 보안 강도는 기반 블록암호 알고리즘의 보안 강도를 준용하였으며, 이는 키 복구 공격에 대한 안전성을 고려한 것이다.

  – 무작위로 선택한 함수와의 구별 공격이나 인증암호화 모드의 태그 위조 공격은 고려하지 않았다.

- ECB 모드는 긴 길이(여러 블록) 데이터의 암호화를 위해 사용하는 것을 금지하므로, 알고리즘 목록에 포함하지 않았다.

- 레거시 환경을 위한 데이터 처리와 기밀성 제공 목적이 아닌 시도-응답 프로토콜 적용 그리고 암호 키와 같은 랜덤한 블록의 암호화에 제한적으로 사용할 수 있다.

● 검증대상이 아닌 기술에 관한 사항은 다음과 같다.

- 암호 알고리즘에 사용하는 키의 보호를 위한 키랩(key wrap) 기술은 NIST SP 800-38F에 블록암호 기반 운영모드 형태로 정의되어 있다. 기반 블록암호로 AES를 사용할 수 있으며, 같거나 유사한 기술이 IETF RFC 3394와 5649, ISO 20038, ANSI X9.102 등에 표준화되어 있다.

- CCM, GCM 외의 인증암호화 표준은 TLS 1.3의 필수 알고리즘인 ChaCha20-Poly1305(RFC 8439/8446), 논스 오용 안전성을 제공하는 AES-GCM-SIV(RFC 8452), 1-pass 구조로 성능이 우수한 OCB3(RFC 7253), 국제표준인 EAX(ISO/IEC 19772) 등이 있으며, 산업계의 실질적 활용도는 ChaCha20-Poly1305가 가장 높다.

- KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제표준 암호 알고리즘을 사용하여야 한다.

## ❷ 해시함수

보안 강도에 따른 해시함수 알고리즘의 사용 정책은 [표 8]과 같다.

**[표 8] 해시함수 보안 강도 기준**

| 알고리즘 | 보안 강도 (충돌 저항성) | 출력 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|
| LSH-224, LSH-512/224, SHA2-224, SHA3-224 | 112비트 | 224비트 | 한시적 허용 | 제한 | 금지 |
| LSH-256, LSH-512/256, SHA2-256, SHA3-256 | 128비트 | 256비트 | 허용◈ | 허용 | |

| 알고리즘 | 보안 강도 (충돌 저항성) | 출력 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|
| LSH-384, SHA2-384, SHA3-384 | 192비트 | 384비트 | 허용◈ | | |
| LSH-512, SHA2-512, SHA3-512 | 256비트 | 512비트 | 허용◈ | | |

- 해시함수의 보안 강도는 충돌 저항성(collision resistance)을 기준으로 정의하였다.
- 보안 강도가 112비트인 해시함수는 2031년부터 사용을 제한하고 2041년부터 사용을 금지한다.
- 양자컴퓨터 기반 암호공격을 고려하여 2031년부터는 보안 강도가 192 또는 256비트인 해시함수의 사용을 권장한다. 이러한 사실이 보안 강도가 128비트인 해시함수의 안전성이 양자컴퓨터 공격으로 저하될 것을 예상한다는 의미는 아니다.
- 검증대상이 아닌 기술에 관한 사항은 다음과 같다.
  - SHA-1 알고리즘의 사용을 제한한다. SHA-1은 ISO/IEC 10118-3에 명시된 해시함수이며, 2024년 검토에서 제외되지 않아 현재 유효한 국제표준이다. 하지만, ISO/IEC 표준에서도 충돌 저항성이 필요한 분야에서 SHA-1의 사용을 제한하고 있다. 더구나 미국은 전자서명 생성을 위한 SHA-1의 사용을 전면 금지하고 레거시 환경에서의 서명 검증에만 사용을 허용하고 있으며, 전자서명이 아닌 분야도 2031년 1월부터 사용을 금지하기로 하였다.
  - KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제표준 암호 알고리즘을 사용하여야 한다.

## ❷ 메시지 인증코드

메시지 인증코드 알고리즘의 보안 강도와 사용 정책은 [표 9], [표 10], [표 11]과 같다.

**[표 9] CMAC 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 블록암호 | 블록암호 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|
| CMAC | 128비트 | HIGHT | 128비트 | 한시적 허용 | 제한 | 금지 |
| | | SEED, LEA-128, ARIA-128, AES-128 | 128비트 | 허용◈ | 허용 | |
| | 192비트 | LEA-192, ARIA-192, AES-192 | 192비트 | 허용◈ | | |
| | 256비트 | LEA-256, ARIA-256, AES-256 | 256비트 | 허용◈ | | |

**[표 10] GMAC 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 블록암호 | 블록암호 키 길이 | 2030년 12월까지 | 2031년 1월부터 |
|---|---|---|---|---|---|
| GMAC | 128비트 | SEED, LEA-128, ARIA-128, AES-128 | 128비트 | 허용◈ | 허용 |
| | 192비트 | LEA-192, ARIA-192, AES-192 | 192비트 | 허용◈ | |
| | 256비트 | LEA-256, ARIA-256, AES-256 | 256비트 | 허용◈ | |

- 메시지 인증코드의 출력인 인증 태그의 길이는 기반 블록암호 또는 해시함수의 출력 길이와 같다고 가정하였다.
- 블록암호 기반 메시지 인증코드의 보안 강도는 기반 블록암호의 보안 강도를 준용한다.
- 블록암호 HIGHT의 사용 정책을 반영하여 이를 사용하는 메시지 인증코드 알고리즘도 2031년부터 사용을 제한하였다.

- 검증대상이 아닌 기술에 관한 사항은 다음과 같다.

  - 블록암호 기반 메시지 인증코드 CBC-MAC의 단독 사용을 금지한다. ISO/IEC 9797-1은 현재도 CBC-MAC을 규정하고 있으나, 메시지 길이를 고정하는 등 제한적인 환경에만 사용하도록 권장하고 있다. NIST는 DES의 폐기에 따라 2008년 블록 길이가 64비트인 CBC-MAC(FIPS PUB 113)을 폐기하였다. 이후 AES 기반 CBC-MAC을 독립적으로 표준화하지 않았고, 그 정의는 CCM 운영모드 명세에만 남아 있다. 이런 이유로 CBC-MAC은 현재도 광범위하게 쓰이고 있으나, NIST는 독립적인 메시지 인증코드로 CBC-MAC의 사용을 금지하고 있다.

  - KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.

- 해시함수 기반 메시지 인증코드 알고리즘인 HMAC의 보안 강도는 기반 해시함수의 보안 강도(충돌 저항성)가 아닌 키 길이로 산정하였다.

- 2031년 1월부터 보안 강도가 112비트인 해시함수의 사용을 제한하므로, 이에 기반한 HMAC의 사용도 제한하였다. 이는 HMAC의 보안 강도 때문이 아니라, 기반 해시함수의 사용 정책을 상속받은 것이다.

**[표 11] HMAC 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 해시함수 | 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|
| HMAC | 128비트 | LSH-224, LSH-512/224, SHA2-224, SHA3-224 | 128비트 | 한시적 허용 | 제한 | 금지 |
| | | LSH-256, LSH-512/256, LSH-384, LSH-512, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512 | 128비트 | 허용◈ | 허용 | |

| 알고리즘 | 보안 강도 | 기반 해시함수 | 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|
| HMAC | 192비트 | LSH-224, LSH-512/224, SHA2-224, SHA3-224 | 192비트 | 한시적 허용 | 제한 | 금지 |
| | | LSH-256, LSH-512/256, SH-384, LSH-512, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512 | | 허용◈ | | |
| | 256비트 | LSH-256, LSH-512/256, LSH-384, LSH-512, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512 | 256비트 | 허용◈ | | |
| | 384비트 | LSH-384, LSH-512, SHA2-384, SHA2-512, SHA3-384, SHA3-512 | 384비트 | 허용◈ | | |
| | 512비트 | LSH-512, SHA2-512, SHA3-512 | 512비트 | 허용◈ | | |

## ❹ 난수발생기

보안 강도에 따른 난수발생기(PRNG)의 사용 정책은 [표 12], [표 13]과 같다.

**[표 12] 블록암호 기반 난수발생기(PRNG) 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 블록암호 | 블록암호 보안 강도 | 2030년 12월까지 | 2031년 1월부터 |
|---|---|---|---|---|---|
| CTR_DRBG | 128비트 | HIGHT | 128비트 | 한시적 허용 | 금지 |
| | | SEED, LEA-128, ARIA-128, AES-128 | 128비트 | 허용◈ | 허용 |

| 알고리즘 | 보안 강도 | 기반 블록암호 | 블록암호 보안 강도 | 2030년 12월까지 | 2031년 1월부터 |
|---|---|---|---|---|---|
| CTR_DRBG | 192비트 | LEA-192, ARIA-192, AES-192 | 192비트 | 허용◈ | |
| | 256비트 | LEA-256, ARIA-256, AES-256 | 256비트 | 허용◈ | |

- 난수발생기에는 항상 충분한 엔트로피를 가진 입력이 공급된다고 가정하였다.
- 난수발생기는 보호(난수생성)의 개념만 있고 처리의 개념이 없어 사용을 제한하는 것과 금지하는 것이 같으므로 모두 금지라고 표시하였다.
- CTR_DRBG의 보안 강도는 기반 블록암호의 보안 강도로 정의하였다.
- 블록암호 알고리즘 HIGHT의 사용 정책에 의해 이에 기반한 CTR_DRBG도 2031년부터 사용을 금지하였다.
- Hash_DRBG와 HMAC_DRBG의 보안 강도는 기반 해시함수의 역상 저항성을 기준으로 정의하였다.

**[표 13] 해시함수 기반 난수발생기(PRNG) 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 해시함수 | 해시함수 역상 저항성 | 2030년 12월까지 | 2031년 1월부터 |
|---|---|---|---|---|---|
| Hash_DRBG, HMAC_DRBG | 224비트 | LSH-224, LSH-512/224, SHA2-224, SHA3-224 | 224비트 | 한시적 허용 | 금지 |
| | 256비트 | LSH-256, LSH-512/256, SHA2-256, SHA3-256 | 256비트 | 허용◈ | 허용 |
| | 384비트 | LSH-384, SHA2-384, SHA3-384 | 384비트 | 허용◈ | |
| | 512비트 | LSH-512, SHA2-512, SHA3-512 | 512비트 | 허용◈ | |

- 2031년 1월부터 보안 강도가 112비트인 해시함수의 사용을 제한하므로, 이에 기반한 Hash_DRBG와 HMAC_DRBG의 사용도 금지하였다. 이는 난수 발생기의 보안 강도 때문이 아니라, 기반 해시함수의 사용 정책을 상속받은 것이다.
- 검증대상이 아닌 기술에 관한 사항은 다음과 같다.
  - NIST는 기존 SP 800-90A에 포함되어 있던 Dual EC-DRBG를 삭제한 SP 800-90A Rev. 1을 2014년에 발표하였다. Dual EC-DRBG는 백도어 존재에 관한 논란으로 현재는 국제 표준에서 제외된 상태이다.
  - KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.

### ❺ 키 유도 함수

키 유도 함수 알고리즘의 보안 강도와 사용 정책은 [표 14], [표 15]와 같다.

- 키 유도 함수의 보안 강도는 기반 메시지 인증코드 알고리즘의 보안 강도로 정의한다.
- 블록암호 알고리즘 HIGHT와 보안 강도가 112비트인 해시함수의 사용 정책을 반영하여 2031년부터 이들을 사용하는 키 유도 함수의 사용을 제한한다. 이는 키 유도 함수의 보안 강도 때문이 아니라, 기반 블록암호와 해시함수의 사용 정책을 상속받은 것이다.
- 키 유도 함수의 보안 강도를 넘어서는 보안 강도가 요구되는 환경에 사용할 키를 생성하는 용도로 사용하지 않아야 한다.

**[표 14] CMAC 기반 키 유도 함수 알고리즘 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 MAC | 기반 블록암호 | 블록암호 보안 강도 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|---|
| KBKDF | 128비트 | CMAC | HIGHT | 128비트 | 한시적 허용 | 제한 | 금지 |
| | 128비트 | | SEED, LEA-128, ARIA-128, AES-128 | 128비트 | 허용◈ | 허용 | |
| KBKDF | 192비트 | CMAC | LEA-192, ARIA-192, AES-192 | | 192비트 | 허용◈ | |
| | 256비트 | | LEA-256, ARIA-256, AES-256 | | 256비트 | 허용◈ | |

**[표 15] HMAC 기반 키 유도 함수 알고리즘 보안 강도 기준**

| 알고리즘 | 보안 강도 | 기반 MAC | 기반 해시함수 | 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|---|
| KBKDF, PBKDF | 128비트 | HMAC | LSH-224, LSH-512/224, SHA2-224, SHA3-224 | 128비트 | 한시적 허용 | 제한 | 금지 |
| | | | LSH-256, LSH-512/256, LSH-384, LSH-512, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512 | | 허용◈ | 허용 | |
| | 192비트 | | LSH-224, LSH-512/224, SHA2-224, SHA3-224 | 192비트 | 한시적 허용 | 제한 | 금지 |
| | | | LSH-256, LSH-512/256, LSH-384, LSH-512, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512 | | 허용◈ | | |

| 알고리즘 | 보안 강도 | 기반 MAC | 기반 해시함수 | 키 길이 | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|---|---|
| KBKDF, PBKDF | 256비트 | HMAC | LSH-256, LSH-512/256, LSH-384, LSH-512, SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512 | 256비트 | 허용◈ | | |
| | 384비트 | | LSH-384, LSH-512, SHA2-384, SHA2-512, SHA3-384, SHA3-512 | 384비트 | 허용◈ | | |
| | 512비트 | | LSH-512, SHA2-512, SHA3-512 | 512비트 | 허용◈ | | |

## ❺ 확장 출력 함수

확장 출력 함수의 보안 강도와 사용 정책은 [표 16]과 같다.

**[표 16] 확장 출력 함수 보안 강도 기준**

| 알고리즘 | 출력 길이 | 보안 강도 (충돌 저항성) | 2030년 12월까지 | 2031년 1월부터 | 2041년 1월부터 |
|---|---|---|---|---|---|
| SHAKE128 | 가변(d) | min(d/2, 128) 비트 | 허용◈ | 허용 | |
| SHAKE256 | 가변(d) | min(d/2, 256) 비트 | 허용◈ | | |

- 확장 출력 함수는 출력 길이가 정해져 있지 않으므로, 보안 강도를 출력 길이 d에 관한 식으로 정의하였다.
- SHAKE128과 SHAKE256은 각각 KECCAK[256], KECCAK[512]를 기반 치환함수(permutation)로 사용하는 스폰지(Sponge) 구조이므로 최대 보안 강도는 각각 128비트, 256비트이다.

- 확장 출력 함수는 KCMVP 검증대상 암호알고리즘에 포함되지 않았지만, 양자내성암호의 내부 구성요소로 활용도가 높고, 추후 KCMVP 검증대상 암호알고리즘에 양자내성암호가 포함될 예정이므로, 이 문서에서 보안 강도 기준을 제시한다.
- KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.

## 제2절 비대칭 키 암호

이 절에서는 비대칭 키 암호를 공개 키 암호화, 전자서명, 키 설정, 하이브리드로 구분하여 알고리즘별 사용 정책을 제시한다.

### ❶ 공개 키 암호화

공개 키 암호화 알고리즘의 보안 강도와 사용 정책은 [표 17]과 같다.

**[표 17] 공개 키 암호화 알고리즘 보안 강도 기준**

| 알고리즘 | 보안 강도 | 공개 키 길이 (비트) | 해시함수 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|---|
| RSAES | 112비트 | 2,048 | SHA2-224, SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | 128비트 | 3,072 | SHA2-256 | 허용 | 한시적 허용 | 금지 |

### ❷ 전자서명

기존 전자서명 알고리즘의 보안 강도와 사용 정책은 [표 18], [표 19], [표 20]과 같다.

**[표 18] 전자서명 RSASSA 보안 강도 기준**

| 알고리즘 | 보안 강도 | 공개 키 길이 (비트) | 해시함수 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|---|
| RSASSA | 112비트 | 2,048 | SHA2-224, SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | 128비트 | 3,072 | SHA2-256 | 허용 | 한시적 허용 | 금지 |

**[표 19] 전자서명 KCDSA 보안 강도 기준**

| 알고리즘 | 보안 강도 | 도메인 변수 길이(비트) | 해시함수 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|---|
| KCDSA | 112비트 | (2,048, 224) | SHA2-224, SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | | (2,048, 256) | SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | 128비트 | (3,072, 256) | SHA2-256 | 허용 | 한시적 허용 | 금지 |

**[표 20] 전자서명 알고리즘(타원곡선 기반) 보안 강도 기준**

| 알고리즘 | 보안 강도 | 타원곡선 | 해시함수 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|---|
| EC-KCDSA/ ECDSA (Prime Field, Binary Field) | 112비트 | P-224<br>B-233<br>K-233 | SHA2-224, SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | 128비트 | P-256<br>B-283<br>K-283 | SHA2-256 | 허용 | 한시적 허용 | 금지 |

양자내성 전자서명 알고리즘의 보안 강도와 사용 정책은 [표 21]과 같다.

**[표 21] 양자내성 전자서명 안전성 범주 기준**

| 암호 구분 | 안전성 범주 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|
| 양자내성 전자서명 | C1, C2 | ※ | 한시적 허용 | |
| | C3, C4, C5 | ※ | 허용 | |

※ 가능한 경우 다른 선택지의 사용을 우선 권장함

- 검증대상이 아닌 기술에 관한 사항은 다음과 같다.

  – 미국 NIST는 2023년에 발표한 FIPS 186-5를 통하여 에드워드 곡선상의 이산대수 문제에 기반한 전자서명 EdDSA를 표준화하였다. 이와 함께, DSA의 사용을 제한하고 이진체(binary field) 상의 타원곡선 기반 전자서명의 사용을 한시적 허용으로 변경하였다. ISO/IEC는 EdDSA를 포함하는 개정 표준 ISO/IEC 14888-3/Amd 1의 제정을 추진 중이다.

**[표 22] 양자내성 전자서명 알고리즘 예시**

| 알고리즘 | 안전성 범주 | 공개 키 길이 (바이트) | 서명 길이 (바이트) | 내부 대칭 키 암호 |
|---|---|---|---|---|
| ML-DSA | C2 | 1,312 | 2,420 | SHAKE128, SHAKE256 |
| | C3 | 1,952 | 3,309 | |
| ML-DSA | C5 | 2,592 | 4,627 | SHAKE128, SHAKE256 |
| SLH-DSA | C1 | 32 | 7,856 | SHA2-256, SHAKE256 |
| | | | 17,088 | |
| | C3 | 48 | 16,224 | SHA2-256, SHA2-512, SHAKE256 |
| | | | 35,664 | |
| | C5 | 64 | 29,792 | SHA2-256, SHA2-512, SHAKE256 |
| | | | 49,856 | |

| 알고리즘 | 안전성 범주 | 공개 키 길이 (바이트) | 서명 길이 (바이트) | 내부 대칭 키 암호 |
|---|---|---|---|---|
| AIMer | C1 | 32 | 4,704 | SHAKE128 |
| | | | 6,944 | |
| | C3 | 48 | 10,320 | SHAKE256 |
| | | | 15,408 | |
| | C5 | 64 | 20,224 | |
| | | | 31,360 | |
| HAETAE | C2 | 992 | 1,474 | SHAKE256 |
| | C3 | 1,472 | 2,349 | |
| | C5 | 2,080 | 2,948 | |

- EdDSA는 보안 강도가 128비트인 Ed25519와 보안 강도가 224비트인 Ed448로 구성되어 있으며, 그 내부에서 각각 SHA-512와 SHAKE256을 사용한다.
- KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.
- 표준화가 되었거나 진행 중인 양자내성 전자서명 알고리즘의 예는 [표 22]에서 확인할 수 있다.

## ❸ 키 설정

### 가. 키 합의

키 합의 알고리즘의 보안 강도와 사용 정책은 [표 23], [표 24]와 같다.

**[표 23] DH 키 합의 보안 강도 기준**

| 알고리즘 | 보안 강도 | 도메인 변수 길이 (비트) | 해시함수 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|---|
| DH | 112비트 | (2,048, 224) | SHA2-224, SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | | (2,048, 256) | SHA2-256 | 허용 | 한시적 허용 | 금지 |
| | 128비트 | (3,072, 256) | SHA2-256 | 허용 | 한시적 허용 | 금지 |

**[표 24] ECDH 키 합의 보안 강도 기준**

| 알고리즘 | 보안 강도 | 타원곡선 해시함수 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|
| ECDH | 112비트 | P-224, B-233, K-233 | 허용 | 한시적 허용 | 금지 |
| | 128비트 | P-256, B-283, K-283 | 허용 | 한시적 허용 | 금지 |

- DH는 파라미터 생성 과정도 검증 항목에 포함되므로 이 과정에 사용하는 해시함수를 지정하여야 한다. 이에 반하여 ECDH는 정해진 타원곡선 파라미터를 사용하므로 별도로 해시함수를 명시할 필요가 없다.
- KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.

### 나. 키 캡슐화 메커니즘(KEM)

키 캡슐화 메커니즘(이하 KEM)의 보안 강도와 사용 정책은 [표 25]와 같다.

**[표 25] 양자내성 KEM 보안 강도 기준**

| 알고리즘 | 보안 강도 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|
| 양자내성 KEM | C1, C2 | ※ | 한시적 허용 | |
| | C3, C4, C5 | ※ | 허용 | |

※ 가능한 경우 다른 선택지의 사용을 우선 권장함

- KEM은 향후 검증대상으로 지정될 예정이며, 검증대상이 아닌 기술에 관한 사항은 다음과 같다.

  – KCMVP 검증대상 암호알고리즘을 사용할 수 없는 경우 국내 또는 국제 표준 암호 알고리즘을 사용하여야 한다.

  – 국내외에서 표준화가 되었거나 진행 중인 양자내성 KEM의 예는 [표 26]에서 확인할 수 있다.

**[표 26] 양자내성 KEM 알고리즘 예시**

| 알고리즘 | 안전성 범주 | 공개 키 길이 (바이트) | 암호문 길이 (바이트) | 내부 대칭 키 암호 |
|---|---|---|---|---|
| ML-KEM | C1 | 800 | 768 | SHA3-256, SHA3-512, SHAKE128, SHAKE256 |
| | C3 | 1,184 | 1,088 | |
| | C5 | 1,568 | 1,568 | |
| FrodoKEM | C1 | 9,616 | 9,752 | SHAKE128, AES128 |
| | C3 | 15,632 | 15,792 | SHAKE256, AES128 |
| | C5 | 21,520 | 21,696 | |
| Classic McEliece | C1 | 261,120 | 96 | SHAKE256 |
| | C2 | 524,160 | 156 | |
| Classic McEliece | C4 | 1,044,992 | 208 | SHAKE256 |
| | C4 | 1,047,319 | 194 | |
| | C5 | 1,357,824 | 208 | |

| 알고리즘 | 안전성 범주 | 공개 키 길이 (바이트) | 암호문 길이 (바이트) | 내부 대칭 키 암호 |
|---|---|---|---|---|
| NTRU | C1 | 699 | 699 | SHA3-256, SHAKE256 |
| | C3 | 930 | 930 | |
| | C3 | 1,138 | 1,138 | |
| | C5 | 1,230 | 1,230 | |
| NTRU+ | C1 | 1,152 | 1,152 | SHAKE256 |
| | C1 | 1,296 | 1,296 | |
| | C3 | 1,728 | 1,728 | |
| SMAUG-T | C1 | 672 | 608 | SHA3-256, SHAKE128, SHAKE256 |
| | C1 | 672 | 672 | |
| | C3 | 1,088 | 992 | |
| | C5 | 1,440 | 1,376 | |

## 제3절 비대칭 키 암호의 하이브리드 사용

하이브리드는 전자서명과 키 설정의 두 가지 기능에 모두 사용되는 방식으로, 두 기능의 하이브리드에 대한 보안 강도와 사용 정책은 [표 27], [표 28]과 같다.

**[표 27] PQ/T 하이브리드의 보안 강도 및 안전성 범주 기준**

| 암호 구분 | 기반 알고리즘 보안 강도 | | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|---|
| | PQ | T | | | |
| PQ/T | C1, C2 | 112비트 이상 | 허용 | 한시적 허용 | |
| | C3, C4, C5 | 112비트 | 허용 | | 한시적 허용 |
| | C3, C4, C5 | 128비트 이상 | 허용◈ | | 한시적 허용 |

**[표 28] PQ/PQ 하이브리드의 안전성 범주 기준**

| 암호 구분 | 기반 알고리즘 보안 강도 | 2030년 12월까지 | 2031년 1월부터 | 2036년 1월부터 |
|---|---|---|---|---|
| PQ/PQ | C1, C2 | ※ | 한시적 허용 | |
| | C3, C4, C5 | ※ | 허용 | |

※ 가능한 경우 다른 선택지의 사용을 우선 권장함

- 하이브리드의 보안 강도는 결합한 두 성분 중 해당 시기의 주된 위협에 대응할 수 있는 성분의 안전성으로 정의한다.
  - 2035년까지는 기존 비대칭 키 암호 성분의 보안 강도로 정의
  - 2036년 1월부터는 양자내성암호 성분의 안전성 범주로 정의
- 하이브리드 KEM은 IETF를 중심으로 표준화를 진행 중이며, 관련 초안은 MLKEM768-P256, MLKEM768-X25519, MLKEM1024-P384 세 가지 하이브리드 KEM을 제시한다.
- 하이브리드 전자서명은 IETF에서 표준화 되었으며, 구성 방식은 다음과 같이 구분한다.
  - 연접(concatenation) 방식 : 두 성분 서명을 각각 생성하여 함께 제시하는 방식
  - 중첩(nesting) 방식 : 한 성분의 서명 결과를 다른 성분의 서명 입력에 포함시켜 계층적으로 생성하는 방식
  - 융합(fused) 방식 : 두 성분을 결합하여 분리할 수 없는 하나의 서명을 생성하는 방식
- 하이브리드를 하이브리드-AND와 하이브리드-OR로 구분하여 언급하는 경우 이 문서의 하이브리드는 하이브리드-AND를 의미한다.
  - 하이브리드-OR 방식은 암호 알고리즘의 안전성만 다루는 이 문서의 관점에서는 '단독 사용'과 같은 것이므로 별도로 고려하지 않는다.

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



# 부 록

# 부 록

## 1. 국내외 암호 정책 동향

### 제1절 국외 주요국의 암호 정책 동향

국외 주요국은 자국의 국가·공공 정보시스템에서 활용할 수 있도록 암호 안전성 기준, 암호체계 전환 정책, 암호모듈 검증 제도 등을 운영하고 있으며, 이를 통해 안전한 암호기술을 활용할 수 있는 정책적 토대를 마련한다.

이 절에서는 미국, 캐나다, 유럽(EU, 독일, 프랑스, 네덜란드, 영국), 일본의 최신 암호 정책 동향을 살펴본다.

#### ❶ 미국

미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 연방 표준 암호 알고리즘과 그 안전성 파라미터를 체계적으로 관리하고 있다. 특히 암호 알고리즘의 사용과 전환 정책을 다루는 지침서인 Transitioning the Use of Cryptographic Algorithms and Key Lengths (NIST SP 800-131A, Rev.3)[57]를 통해 보안 강도 기반의 암호 사용 기준을 명확히 안내하고 있다. 각 암호 알고리즘을 허용(acceptable), 비권장(deprecated), 금지(disallowed), 제한(legacy use) 네 가지 상태로 구분하고, 상태를 전환하는 시점과 조건을 구체적으로 명시하였다. NIST는 이를 통해, 암호서비스의 공급자와 사용자 모두에게 안전한 암호의 기준을 제공하고, 그에 따른 암호 보안 강도 상향 및 알고리즘의 전면 전환을 미리 준비할 수 있도록 하였다. 한편, 2026년에는 Securing the Nation Against Advanced Cryptographic Attacks(행정명령 14412)[61]가 발효되어 연방기관의 양자내성암호 전환 일정이

국가 정책으로 명문화되었다.

미국의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 29]와 같다.

**[표 29] 미국의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 최소 보안 강도는 현재 112비트이며, 2031년부터 128비트로 상향 예정. 다만 적용 방식은 알고리즘별로 상이함 |
| 블록암호 | • AES-128/192/256비트의 키 길이 모두 허용<br>• TDEA는 암호화 사용 금지. 기존 데이터 복호화 용도로만 사용 제한 |
| 해시함수 | • SHA-1 및 224비트 해시함수는 2030년까지 비권장, 2031년부터 암호학적 보호에 사용 금지<br>• 그 외 SHA-2와 SHA-3는 모두 허용 |
| 운영모드 | • ECB 모드의 암호화 사용 금지. 기존 데이터의 복호화 용도로만 사용 제한 |
| 비대칭 키 암호 | • 보안 강도 128비트로의 중간 상향 없이 기존 보안 강도 112비트 비대칭 키 암호의 사용을 2030년까지 허용, 2031년 1월부터 비권장 상태로 사용 연장<br>• 2036년 1월부터 기존 비대칭 키 암호는 보안 강도에 상관없이 전면 금지되며, 양자내성암호로 전환하는(one-step) 방식 추진 |
| 전자서명 | • DSA의 사용 제한(신규 서명 생성 금지, 기존 서명 검증 가능) |
| 전환 정책 | • 양자컴퓨터 위협을 고려한 양자내성암호 알고리즘 ML-KEM, ML-DSA, SLH-DSA 표준화 완료<br>• 행정명령 14412에 따라 연방기관 고가치자산 · 고영향시스템 대상 키 설정은 2030년, 전자서명은 2031년까지 전환 의무화 |

## ❷ 캐나다

캐나다는 사이버보안센터(Canadian Centre for Cyber Security, CCCS)가 암호 안정성 기준과 양자내성암호 전환 로드맵을 함께 관장하는 단일기관 체계를 운영한다. CCCS는 지침서 Cryptographic algorithms for UNCLASSIFIED, PROTECTED A and PROTECTED B information(ITSP.40.111)[32]을 통해

**[표 30] 캐나다의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 전체를 아우르는 단일 최소 보안 강도 기준은 없고, 알고리즘별로 개별 요구치를 제시<br>• HMAC, KMAC 키 길이 및 난수발생기(DRBG) 초기 시드 엔트로피는 현재 112비트 이상을 요구하며 2030년까지 128비트 이상으로 상향 |
| 블록암호 | • AES-128/192/256비트를 권장 |
| 해시함수 | • SHA-2, SHA-3 계열을 권장하되, SHA2-224와 SHA3-224는 2030년까지 단계적 폐지 예정<br>• SHA-1은 전자서명 · 충돌저항성이 필요한 용도에는 사용을 금지하며, HMAC · 키 유도 · 난수생성 등 그 외 용도에서는 시한 없이 단계적 폐지 대상 |
| 운영모드 | • 기밀성 보호에는 CFB, OFB, CTR, CBC 모드를 권장하며, 저장매체 보호에는 XTS-AES 모드를 권장<br>• 인증암호화(AEAD)에는 CCM, GCM을 권장<br>• ECB 모드는 단일 블록 암호화나 키래핑 등 특수 용도로만 제한적 허용하고 대량 데이터 암호화에는 사용 금지 |
| 공개 키 암호화 및 키 설정 | • RSA, 유한체 기반 DH/MQV는 최소 2,048비트를 요구하며 2030년까지 3,072비트로 상향<br>• 타원곡선은 P-256, P-384, P-521을 권장하고 P-224 및 이진곡선은 2030년까지 단계적 폐지<br>• 양자내성 KEM은 ML-KEM(FIPS 203)을 범용 메커니즘으로 권장<br>• RSA, 유한체 기반 DH/MQV, 타원곡선 기반 CDH/MQV는 단독 사용 시 2035년까지 단계적 폐지 |
| 전자서명 | • RSA(RSASSA-PKCS1-v1.5 또는 RSASSA-PSS)를 권장하며 2030년까지 3,072비트로 상향<br>• ECDSA는 P-256, P-384, P-521을 권장하고 P-224 및 이진곡선은 2030년까지 단계적 폐지<br>• EdDSA(Edwards25519, Edwards448)를 권장<br>• DSA는 2030년까지 단계적 폐지<br>• RSA, ECDSA, EdDSA는 단독 사용 시 2035년까지 단계적 폐지<br>• 양자내성 서명은 ML-DSA(FIPS 204)와 SLH-DSA(FIPS 205)를 범용 서명으로 권장하며, 개인 키 상태 관리가 가능한 경우에 한해 LMS, XMSS 등 해시 기반 서명도 허용 |

| 항목 | 주요 내용 |
|---|---|
| 전환 정책 | • 2026년 4월까지 부처별 초기 PQC 전환계획 수립 및 매년 진행 상황 보고 개시<br>• 2027년 4월까지 전환계획 갱신, 2028년 4월까지 암호 자산 인벤토리 갱신 완료 및 전환 개시<br>• 2031년까지 고우선순위 시스템 전환 완료, 2035년까지 나머지 시스템 전환 완료<br>• "harvest now, decrypt later" 위협에 노출된 시스템을 우선순위로 지정 권고 |

암호 알고리즘과 키 길이·운영모드 등 사용 방식을 정의하고, 알고리즘을 권장(recommend)과 단계적 폐지(phase out) 두 상태로 구분하며 필요시 알고리즘별로 폐지 시한을 명시한다. 한편, 양자내성암호 전환은 별도 문서인 Roadmap for the migration to post-quantum cryptography for the Government of Canada(ITSM.40.001)[31]에서 다루며, 2026년 4월 부처별 전환계획 수립을 시작으로 2031년 고우선순위 시스템, 2035년 나머지 시스템의 전환 완료라는 국가 목표시한을 제시한다. 이 로드맵은 본래 권고사항이었으나, 2025년 10월 발효된 재무위원회사무처(Treasury Board of Canada Secretariat, TBS)의 정책이행공지(Security Policy Implementation Notice)[60]로 인해 의무 준수사항으로 격상되었다.

캐나다의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 30]과 같다.

### ❸ 유럽

유럽은 EU 차원의 공통 인증체계와 개별 회원국의 독자적인 기술기준이 병존하는 다층적 구조를 갖는다. 각 회원국 대표로 구성된 자문위원회(European Cybersecurity Certification Group, ECCG)가 보안 인증 체계에 적용되는 공통 암호기준을 정하는 한편, 독일·프랑스·네덜란드는 각각 BSI·ANSSI·NCSC-NL을 통해 자국 공공부문에 적용되는 별도의 기준을 운영한다. 두 체계는 상호 배타적이지 않고 목적(인증 vs. 자국 공공부문 지침)에 따라 병행

적용된다. 이 절에서는 EU 공통기준에 이어 독일·프랑스·네덜란드의 국가별 기준을 살펴보고, EU 비회원국인 영국의 기준까지 함께 검토한다.

## 가. 유럽연합(EU)

유럽연합(EU)은 단일 표준 중심의 미국과 달리, 보안 인증 체계(EU Cybersecurity Certification, EUCC)를 기반으로 다양한 암호기술을 허용하는 정책을 시행하고 있다. 유럽연합 사이버보안청 ENISA는 EUCC를 설계하며, 각 회원국 대표로 구성된 자문위원회인 ECCG의 협의를 거쳐 운영한다. ECCG 산하에는 암호 분야를 전담하는 암호 소위원회(Sub-group on Cryptography)가 별도로 설치되어 있으며, 이 소위원회는 Agreed Cryptographic Mechanism[35]를 통해 보안 인증 체계에서 허용하는 암호 알고리즘 목록과 권장 보안 수준을 정의한다.

해당 문서에서는 암호 알고리즘을 안전성 기준에 따라 권장(recommended)과 조건부허용(admissible) 두 가지 상태로 구분하고, 알고리즘별로 사용 제한 시점을 안내하고 있다. 2025년의 버전 2.0과 달리, 2026년 4월에 공개된 버전 3.0 초안은 기존 상태 중 '제한(legacy)'을 '조건부허용(admissible)'으로 변경하고, 양자내성암호 전환을 위한 구조적 개편을 담았다. 신규 시스템에는 권장 메커니즘의 적용이 원칙이며, 조건부허용 메커니즘을 적용하고자 하는 경우 하위호환성 등 정당한 사유가 필요하다. 이 문서는 2년 주기로 검토·개정하도록 규정되어 있다.

유럽연합의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 31]과 같다.

**[표 31] 유럽연합의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 권장 메커니즘은 최소 125비트 이상의 보안 강도를 요구<br>• 조건부허용 메커니즘은 유효기간을 부여해 관리하며(기본 2033년 이후까지), 조기 취약화가 예상되는 경우 단계적 폐지 대상<br>• 신규 시스템은 권장 메커니즘 사용이 원칙이며, 조건부허용 사용 시 하위 호환성 등 정당한 사유 제시를 요구 |
| 블록암호 | • AES-128은 조건부허용, AES-192/256은 권장<br>• 양자컴퓨터 공격을 고려하는 환경에서는 192비트 이상을 권장하되, Grover 알고리즘의 현실적 제약으로 키 길이를 무조건 2배 확장할 필요는 없음 |
| 해시함수 | • SHA-2와 SHA-3 계열을 ECCG 승인 목록으로 하며, 출력길이 256비트는 조건부허용, 384비트 이상은 권장. 양자컴퓨터 공격을 고려하는 환경에서는 384비트 이상 출력 길이를 권장<br>• SHA-1은 ECCG 승인 목록에서 제외하며, 예외적으로 HMAC-SHA-1만 2030년까지 조건부허용<br>• 224비트 해시함수는 2026년 1월부터 ECCG 승인 목록에서 제외<br>• 신규 항목으로 확장 출력 함수(XOF)를 도입하여 SHAKE256/cSHAKE256은 권장, SHAKE128/cSHAKE128은 조건부허용으로 구분 |
| 운영모드 | • 인증암호화는 Encrypt-then-MAC, CCM, GCM, EAX를 권장<br>• MAC-then-Encrypt와 Encrypt-and-MAC은 2026년 1월부터 ECCG 승인 목록에서 제외 |
| 비대칭 키 암호 | • 기존 비대칭 키 암호는 보안 강도에 상관없이 모두 조건부허용<br>• 양자컴퓨터 공격을 고려하는 환경에서는 단독 사용이 금지되고 양자내성 암호와의 하이브리드(PQ/T Hybrid) 방식이 요구됨 |
| 양자내성 암호 | • 격자 기반 양자내성 메커니즘(ML-KEM, FrodoKEM, ML-DSA 등)은 아직 충분히 검증되지 않았기에 단독 사용을 지양하고, 기존 방식과의 하이브리드를 권장<br>• 해시 기반 서명(XMSS, LMS, SLH-DSA 등)은 하이브리드가 선택사항이며, 단독 사용도 허용됨 |
| 전환 정책 | • 장기간 보호가 필요한 응용 분야를 우선 대상으로, “harvest now, decrypt later” 공격에 대응하기 위해 하이브리드 방식 사용을 권고<br>• 모든 시스템의 일괄 전환보다는 응용 환경과 데이터 보호 기간에 따라 우선순위를 구분하는 차별적 전환 정책을 채택 |

| 항목 | 주요 내용 |
|---|---|
| 전환 정책 | • ECCG와는 별도로, 유럽집행위원회의 권고에 따라 NIS 협력그룹(NIS CG)이 회원국 공통 전환 일정을 제시함<br>• 2026년까지 초기 조치 이행 및 국가별 전환계획 수립, 2030년까지 고위험 응용 분야 전환 완료, 2035년까지 중위험 분야 전환 완료·저위험 분야는 가능한 범위에서 완료 권고 |

## 나. 독일

독일 연방정보기술보안청(Bundesamt für Sicherheit in der Informationstechnik, BSI)의 암호 정책은 암호 알고리즘과 키 길이 권고를 넘어, 구현 관점의 보안과 실제 암호가 적용되는 환경까지 고려한 실무 중심의 보안 기준을 제시하고 있다. BSI는 지침서 Cryptographic Mechanisms: Recommendations and Key Lengths(BSI TR-02102-1)[28]를 통해 전체 최소 보안 강도 기준인 120비트를 선언한 뒤, 블록암호·해시함수·비대칭 키 암호·전자서명 등 범주별로 이 기준을 충족하는 구체적인 권장 알고리즘과 키 길이를 제시한다. 해당 지침서는 매년 개정되고 있으며, 2026년 1월에 개정된 지침서에서는 양자컴퓨터 위협에 대응하기 위해 처음으로 구체적인 전환 시한을 도입하고, 기존 비대칭 키 암호의 단독 사용을 중단하도록 명시하였다.

독일의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 32]와 같다.

**[표 32] 독일의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 모든 암호 메커니즘의 보안 강도는 최소 120비트 권장 |
| 블록암호 | • AES-128/192/256을 권장<br>• 신규 암호 응용체계에서는 블록크기 128비트 이상인 블록암호만 사용. 높은 수준의 보안이 필요하거나 장기적인 보호가 요구되는 응용 등의 경우에는 256비트 키 길이 사용 권장 |

| 항목 | 주요 내용 |
|---|---|
| 해시함수 | • 256비트 출력길이 이상의 SHA-2와 SHA-3 사용 권장<br>• SHA-1은 사용 금지하며, HMAC 등 부수 용도의 사용도 지양<br>• 높은 수준의 보안이 필요하거나 장기적인 보호가 요구되는 응용 등의 경우에는 최소 384비트 출력길이의 해시함수 사용 권장 |
| 운영모드 | • 데이터 인증이 없는 경우에는 CBC, CTR을 권장<br>• 인증암호화(AEAD) 경우는 CCM, GCM, AES-GCM-SIV를 권장<br>• GCM, CCM 사용 시 인증태그 길이 96비트 이상을 권장하며, 논스(nonce) 재사용 우려가 있는 경우 AES-GCM-SIV 사용 권장 |
| 공개 키 암호화 및 키 설정 | • 기존 비대칭 키 암호는 RSA, DLIES, DH에 대해 3,000비트, ECIES, ECDH에 대해 250비트의 키 길이를 권장하며, 단독 사용은 2031년까지 권장<br>• 양자내성 KEM은 성숙도 미비, 부채널 등 미발견 결함 가능성으로 인해 단독 사용을 권장하지 않으며, 기존 방식과 결합한 하이브리드 방식을 권장<br>• 하이브리드 방식은 CatKDF(KMAC 또는 HKDF 병행), KeyCombine을 권장 |
| 전자서명 | • 기존 서명 방식 중 DSA는 2029년까지만 권장. 그 외 기존 서명 방식은 2035년까지 사용을 권장<br>• RSA 서명의 키 길이는 최소 3,000비트, 타원곡선 서명의 키 길이는 최소 250비트 권장<br>• 2036년 1월부터 양자내성 서명으로 전환(ML-DSA는 하이브리드 형태, SLH-DSA 등 해시 기반은 단독 가능) |
| 전환 정책 | • 기존 키합의(키 설정) 방식의 단독 사용은 2031년까지 권장하고, 매우 높은 보호 수준이 요구되는 경우는 2030년까지 조기 전환을 권장<br>• 전자서명은 2035년까지 기존 방식 사용 후 하이브리드 및 양자내성 서명으로 전환<br>• 하이브리드 방식을 지원하기 위한 키 조합기(key combiner) 메커니즘을 권장 목록에 신규로 포함 |

## 다. 프랑스

프랑스는 사이버보안청(Agence nationale de la sécurité des systémes d'information, ANSSI)이 암호 정책을 총괄한다. ANSSI는 지침서 Régles et recommandations concernant le choix et le dimensionnement des

mécanismes cryptographiques(ANSSI-PG-083)[23]를 통해 암호 메커니즘의 공격 복잡도, 키 길이, 파라미터 크기 및 안전성 가정에 관한 요구사항을 반드시 준수해야 하는 규칙(régles)과 모범사례에 해당하는 권고(recommandations)로 구분하여 제시한다. 2026년 3월 개정된 지침서에서는 양자위협을 반영하고, 기존 규칙·권고 체계에 추가로 양자내성 안전성을 목표로 할 때 적용되는 별도의 규칙과 권고 체계를 신설하였다.

프랑스의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 33]과 같다.

**[표 33] 프랑스의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 대칭 키는 최소 128비트를 요구<br>• 양자내성을 목표로 할 경우 192비트 이상을 권장 |
| 블록암호 | • 블록크기는 최소 128비트를 요구<br>• AES-128은 규칙을 충족하며, AES-192/256은 양자내성 권고까지 충족 |
| 해시함수 | • 출력길이 최소 256비트를 요구<br>• 양자내성을 목표로 할 경우 384비트 이상을 권장 |
| 비대칭 키 암호 | • RSA, 유한체 기반 이산대수는 2030년까지 최소 2,048비트, 2031년부터 최소 3,072비트를 요구<br>• 타원곡선에 대해서는 부분군 위수 최소 250비트를 요구<br>• 이 기준은 암호화·키 설정·전자서명에 공통 적용 |
| 양자내성 암호 | • 양자내성 KEM의 단독 사용은 인정되지 않으며, 기존 비대칭 키 암호와 결합한 하이브리드 방식이 필수<br>• 전자서명의 경우 ML-DSA는 하이브리드 방식이 필수인 반면, SLH-DSA는 해시 기반 구조이므로 하이브리드 없이도 단독 사용 가능 |
| 전환 정책 | • 2030년 1월 1일 이후에도 사용 예정이거나 “harvest now, decrypt later” 공격 위험이 있는 메커니즘에는 양자내성 안전성을 지향할 것을 권고<br>• 2027년부터 일부 인증 대상 제품에 양자내성암호 탑재를 의무화할 예정이며, 지침서 개정 주기도 기존 2년에서 2~5년으로 조정 |

## 라. 네덜란드

네덜란드는 단일 기술표준기관이 암호기준을 총괄하는 미국·독일과 달리, 정책부처와 기술기관이 역할을 나눈 이원적 체계를 운영한다. 국가 암호정책 프레임워크인 Rijksbreed beleidskader cryptografie[42]는 부처간 업무운영위원회(Interdepartementale Commissie Bedrijfsvoering Rijk, ICBR)가 확정한다. 2025년 2월 확정된 이 프레임워크(버전 1.0)는 중앙정부 기관에 대해 암호정책에 반드시 포함해야 할 항목을 규정하나, 암호 강도나 키 길이 등 구체적인 수치는 제시하지 않는다. 실질적인 기준 문서 역할을 하는 것은 국가사이버보안센터(Nationaal Cyber Security Centrum, NCSC-NL)의 TLS 보안지침인 Transport Layer Security (TLS) Security guidelines[51]이며, 알고리즘 및 설정마다 좋음(Goed), 충분(Voldoende), 단계적 폐지(Uit te faseren), 불충분(Onvoldoende) 4단계로 등급을 구분한다. 한편, 양자내성암호 전환 방법은 이 TLS 지침의 별도 절과, AIVD·CWI·TNO가 공동 발간한 PQC Migration Handbook[22]에서 제시한다.

네덜란드의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 34]와 같다.

**[표 34] 네덜란드의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 좋음·충분 등급은 최소 128비트, 단계적 폐지 등급은 최소 112비트의 암호학적 강도를 요구<br>• 양자컴퓨터가 기존 공개 키 암호를 무력화할 수 있는 시점(CRQC 실현 시점)을 2030~2040년으로 전망 |
| 블록암호 및 운영모드 | • AES-256-GCM을 좋음 등급으로 권장<br>• (참고) 스트림 암호 ChaCha20-Poly1305도 좋음 등급으로 권장<br>• AES-256-CCM, AES-128-GCM, AES-128-CCM은 충분 등급<br>• AES-CBC 계열(128, 256비트)과 CAMELLIA·ARIA는 단계적 폐지 대상 |
| 해시함수 | • SHA-512, SHA-384, SHA-256을 좋음 등급으로 권장<br>• SHA-224는 단계적 폐지 대상 |

| 항목 | 주요 내용 |
|---|---|
| 해시함수 | • SHA-1, MD5는 사용 금지(불충분) |
| 공개 키 암호화 및 키 설정 | • 기존 ECDHE는 충분, DHE는 단계적 폐지로 하향<br>• 키교환은 양자내성 하이브리드 알고리즘(X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024)을 최초로 좋음 등급으로 지정 |
| 전자서명 | • ECDSA, RSA-PSS, EdDSA는 양자위협을 반영해 최고등급에서 한 단계 하향된 충분 등급으로만 인정하며, 좋음 등급은 부여하지 않음<br>• RSA는 최소 3,072비트를 충분 등급으로 요구, RSA-PSS 패딩 사용 전제<br>• 양자내성 서명 알고리즘은 아직 TLS 표준에 포함되지 않아 선택지 없음 |
| 전환 정책 | • AIVD·CWI·TNO가 공동 발간한 PQC Migration Handbook은 고정된 국가 시한 대신 Mosca의 부등식에 기반한 조직별 위험평가 방식 채택<br>• 양자컴퓨터의 공개 키 암호 위협 시점을 늦어도 2040년, 빠르면 2030년으로 추정하며 전체 전환에 5년 이상 소요될 수 있다는 점에서 조기 대응 권고<br>• “harvest now, decrypt later” 공격 위협에 노출된 조직에는 즉시 전환 준비 착수 권고<br>• 알고리즘 파라미터는 가능한 경우 최고 보안수준(NIST 안전성 범주 5)을 권장하며, 서명은 보안수준 5 또는 3을 목표 |

## 마. 영국

영국은 국가사이버보안센터(National Cyber Security Centre, NCSC-UK)가 암호기준과 양자내성암호 전환 시한을 함께 관장하는 단일기관 체계를 운영한다. 네덜란드처럼 정책부처와 기술기관이 분리되거나, 독일처럼 여러 문서가 위계를 이루는 구조 없이, NCSC-UK가 TLS, IPsec 등 프로토콜별 기술지침과 PQC 전환 시한을 모두 직접 발간한다. 이 가운데 TLS 설정 기준을 제시하는 Using TLS to protect data[53] 문서를 중심으로 영국의 암호 안전성 기준을 요약한다. 이 문서는 네덜란드·독일처럼 여러 알고리즘을 등급별로 나열하는 방식이 아니라 TLS 버전별로 소수의 권장 프로파일(Recommended Profile)을 지정하는 방식을 취한다. 한편, 양자내성암호 전환은 별도 문서인 Timelines for migration to post-quantum cryptography[52]에서 다루며,

2028 · 2031 · 2035년의 구체적인 국가 목표시한을 명시한다.

영국의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 35]와 같다.

**[표 35] 영국의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 별도의 보안 강도 등급 체계 없이, 권장 프로파일 자체가 128비트로 고정 |
| 블록암호 및 운영모드 | • AES-128-GCM을 TLS 1.3, 1.2 권장 프로파일의 유일한 암호화 방식으로 지정<br>• CBC 모드는 AES-GCM을 지원하지 않는 구현을 위한 TLS 1.2 호환성 프로파일에서만 허용 |
| 해시함수 | • SHA-256을 권장 프로파일의 표준 해시로 지정<br>• SHA-1은 TLS 1.0, 1.1 등 구버전에서만 남아있으며, 사용 지양 |
| 공개 키 암호화 및 키 설정 | • 키교환은 ECDHE(P-256 곡선)로 고정<br>• 인증은 ECDSA(P-256, SHA256) 또는 RSA(2048비트, SHA256) 중 하나를 쓰는 두 프로파일만 제시<br>• 인증서 발급 시에도 동일 파라미터 권장 |
| 전환 정책 | • 2028년까지 암호자산 전수조사 · 전환계획 수립<br>• 2031년까지 최우선순위 시스템 전환 완료<br>• 2035년까지 전체 시스템 · 서비스 · 제품 PQC 전환 완료라는 3단계 국가 목표시한 공식 제시<br>• TLS 1.2는 PQC를 지원하지 않으므로 TLS 1.3으로의 전환 계획 수립을 권고 |

## ❹ 일본

일본의 암호 정책은 디지털청 · 총무성 · 경제산업성이 전문가 협의체인 암호기술평가위원회(Cryptography Research and Evaluation Committees, CRYPTREC)를 통해 운영하는 두 가지 지침서를 중심으로 이루어진다. 첫째는 구체적 알고리즘 목록을 규정하는 List of Ciphers to be Referred to in Procurement for e-Government(CRYPTREC Cipher List)(CRYPTREC LS-0001-2022R2)[33]이고, 둘째는 그 알고리즘의 운용기간별 필요 보안

강도 및 키 길이 산정 방법론을 규정하는 Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection(CRYPTREC LS-0003-2022r1)[34]이다. 시스템의 운용 기간과 데이터 보호기간을 조달·개발 기관이 직접 산정하여 그에 맞는 보안 강도를 설정하도록 의무화하며, 통신·저장·전자서명 등 사용 목적별로 보안 강도 기준을 구분하는 것이 특징이다. 한편 2025년 11월 일본 정부가 Migration to Post-Quantum Cryptography (PQC) at Government Agencies, etc.(Interim Report)[43]를 통해 처음으로 2035년을 목표 시한으로 하는 PQC 전환 방침을 제시하였으며, 2026년도 중 구체적인 이행 로드맵을 수립할 예정이다.

일본의 암호 보안 강도 및 알고리즘 사용에 관한 정책을 정리하면 [표 36]과 같다.

**[표 36] 일본의 암호 보안 강도 및 알고리즘 사용에 관한 정책**

| 항목 | 주요 내용 |
|---|---|
| 보안 강도 | • 신규 암호보호 적용 시 2040년까지 128비트 이상, 2041년 이후 192비트 이상 요구<br>• 기존 시스템과의 호환성 유지나 암호학적 처리 목적에 한해 2030년까지 112비트, 2050년까지 128비트 사용을 예외적으로 허용 |
| 블록암호 | • 블록암호는 AES, Camellia를 전자정부 추천암호로 지정 |
| 해시함수 | • 224비트의 출력길이를 제외한 SHA-2, SHA-3를 전자정부 추천암호로 지정<br>• 확장 출력 함수(XOF)로 SHAKE128, SHAKE256을 전자정부 추천암호로 지정 |
| 운영모드 | • 비밀성 보호에는 CBC, CFB, CTR, OFB를 권장하며, 저장매체 암호화 한정으로 XTS를 권장<br>• 인증암호화(AEAD)에는 CCM, GCM을 권장<br>• 메시지인증코드(MAC)는 CMAC, HMAC을, 인증암호는 ChaCha20-Poly1305를 별도로 지정 |
| 공개 키 암호화 및 키 설정 | • 키공유는 DH, ECDH를, 암호화는 RSA-OAEP를 지정<br>• 2026년 3월 CRYPTREC 암호리스트 개정을 통해 양자내성 KEM인 ML-KEM이 전자정부 추천암호 리스트에 최초로 추가됨 |

| 항목 | 주요 내용 |
|---|---|
| 공개 키 암호화 및 키 설정 | • ML-KEM에는 [보안 강도] 항목의 비트 수 기준이 아직 적용되지 않으며, CRYPTREC이 이에 대한 별도 기준 마련을 검토 중 |
| 전자서명 | • ECDSA, EdDSA, RSA-PSS, RSASSA-PKCS1-v1_5를 전자정부 추천 암호로 지정<br>• DSA는 미국 NIST가 FIPS 186-5에서 이미 폐지했으나, 안전성 · 이용실적에 큰 변화가 없다는 이유로 전자정부 추천암호 리스트에 계속 유지<br>• 양자내성 서명 알고리즘은 아직 PQC 리스트에 반영되지 않았으며, CRYPTREC이 추가를 검토 중 |
| 전환 정책 | • 원칙적으로 2035년까지 PQC 전환을 완료하는 것을 목표<br>• 전환 대상은 주로 공개 키 암호이며, 공통키 암호 · 해시함수도 키 길이 상향 검토 대상에 포함<br>• 2026년도 중 구체적 이행 로드맵 수립 예정이며, 민감정보 · 장기보호 필요 시스템은 "harvest now, decrypt later" 공격 위협을 고려해 조기 전환 검토를 권고 |

## 제2절 국내 암호 정책 동향

우리나라의 암호 정책은 국제 표준 기술을 수용하면서도 핵심 암호 알고리즘은 국내 기술을 우선시하여 기술 주권을 확보하는 방향을 취하고 있다. 특히 국가 · 공공기관이 도입하는 상용 암호모듈에 대해서는 암호 알고리즘의 선택뿐만 아니라 암호의 구현과 모듈의 동작 과정 전반의 적합성을 국가 주도로 검증하는 제도를 운용한다. 이를 통해 암호기술의 선택부터 구현 · 운용에 이르는 전 과정을 정책적으로 관리한다는 점에서 국내 암호 정책은 다른 나라와 구별되는 특징을 가진다.

## ❶ 암호 사용 정책

국가·공공 영역의 암호 알고리즘 사용기준은 국가정보원이 2009년 발간, 국가·공공기관에 배포한 『국가·공공기관 암호 사용 기준』[3]에서 제시하고 있다. 이 기준은 배포 당시 비밀 등 비공개 정책이 포함되어 있어 국가·공공기관 대상으로만 대외비로 배포되었다.

이 기준은 국가·공공기관의 암호제품 도입·사용과 관련, 단계별 고려요소를 제시함으로써, 해당 기관 업무환경에 맞는 최적의 암호기술을 도입·사용할 수 있도록 하기 위해 제정되었다. 즉, 국가·공공기관의 비밀 또는 행정정보 보호를 위한 암호기술 사용과 관련, 준수해야 할 정책·기술적 기준을 제시하고 있다. 특히, 국가·공공기관이 암호기술 도입 검토 단계부터 보안적합성 검증 의뢰 등을 통한 도입 완료까지 절차별 이행 방안을 제시하였다. 이와 더불어 행정기관 표준 암호 알고리즘 목록과 함께 정보의 보안등급별 암호사용 기준을 명시하였다.

민간 영역의 암호 알고리즘 사용 기준은 과학기술정보통신부와 한국인터넷진흥원(KISA)이 발간한 『암호 알고리즘 및 키 길이 이용 안내서』가 제시하고 있다. 이 안내서는 2009년 처음 제정되었으며, 2018년에 개정되었다.

이 안내서는 암호 알고리즘을 크게 대칭 키 암호, 해시함수, 공개 키 암호의 세 가지로 분류하여 권고 알고리즘을 안내하고 있다. 대칭 키 암호로는 ARIA, LEA 등 국내 표준 블록암호를 AES와 함께 권고하고 있다. 해시함수는 그 사용 목적에 따라 메시지인증·키 유도·난수생성 용도와 해시·전자서명 용도로 구분하고, 용도에 따른 권고 알고리즘을 안내하였다. 더불어 SHA-1과 HAS-160 등 보안 강도가 저하된 알고리즘의 사용을 제한하는 정책을 안내하였다. 공개 키 암호는 다양한 보안 강도를 제공하기 위한 키의 길이를 기반 문제에 따른 암호 알고리즘별로 안내하고 있다.

## ❷ 암호모듈 검증 정책

우리나라는 국가기관과 공공기관이 암호모듈을 사용하고자 할 경우, 국가정보원이 안전성을 검증한 암호모듈을 도입하여 사용할 수 있도록 KCMVP를 운영하고 있다. 이 제도는 미국의 CMVP(cryptographic module validation program)와 유사하지만, 국내에서 개발한 암호 알고리즘의 사용을 권장하여 국내 암호산업 보호와 기술 발전의 밑거름이 되어왔다. 최근에는 AES를 검증대상에 추가하여 더 다양한 정보보호 제품에 검증된 AES 암호모듈이 적용될 수 있도록 하여 국가 도입을 장려하고 있고, 양자내성암호의 검증을 준비하여 다가올 위협에 선제 대응하고 있다.

국가정보원은 전자정부법 시행령과 사이버안보 업무규정, 그리고 암호모듈 시험 및 검증 지침을 근거로 KCMVP를 시행하고 있다. 또한, 국가정보원과 국가보안기술연구소가 발간한 『암호모듈 구현안내서 Part 1 : 시험 및 구현 사례별 해설서』와 『암호모듈 구현안내서 Part 2 : 검증대상 암호알고리즘 구현 안내서』[5]를 실무 지침서로 활용하여 암호모듈 자체의 안전성과 함께 암호알고리즘의 구현 적합성을 검증하고 있다.

두 권의 구현안내서 중 『암호모듈 구현안내서 Part 2 : 검증대상 암호알고리즘 구현안내서』는 KCMVP 검증대상 암호 알고리즘의 국내외 참조 표준을 안내하고, 암호 알고리즘 자체가 이론적으로는 안전하더라도 구현 방식에 따라 치명적인 취약점이 발생할 수 있다는 점을 전제로 각 알고리즘의 입력값 조건 검증, 내부 데이터의 처리, 예외 처리 방식 등을 구체적으로 안내한다. 그리고 검증대상 암호 알고리즘을 포함한 암호모듈이 KCMVP 검증을 통과하기 위해 반드시 준수해야 할 구현물 관점의 보안 요구사항을 명확히 안내하고 있다.

이 구현안내서의 의미는 검증대상 암호 알고리즘의 단순 안내와 기술설명에 그치지 않고, 이를 구현하였을 때 발생할 수 있는 실질적인 보안 취약점을 예방하는 데 도움을 준다는 것이며, 이를 통해 우리나라 국가 · 공공기관이 안전한 암호기술을 도입할 수 있도록 하는 중요한 역할을 하고 있다.

## 2. 주요 암호기술 소개

이 절에서는 암호기술을 대칭 키 암호와 비대칭 키 암호로 구분하여 소개한다. 각 기술의 간략한 설명과 함께 KCMVP 검증대상 암호알고리즘 위주로 국내외 참조 표준도 소개한다. 아직 KCMVP 검증대상 암호알고리즘으로 지정되지 않은 양자내성암호의 경우 표준화가 완료되었거나 진행 중인 국내외 주요 알고리즘을 다룬다.

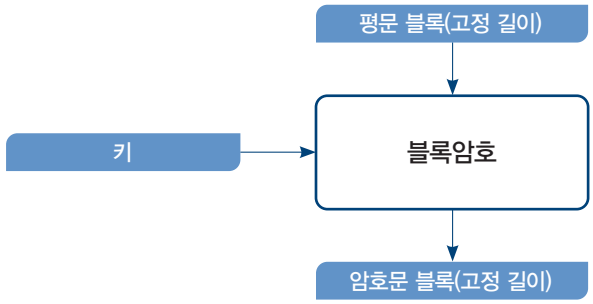
### 제1절 대칭 키 암호

대칭 키 암호(symmetric key cryptography)는 데이터의 암호학적 보호와 처리에 같은 키를 사용하는 암호기술을 통칭한다. 블록암호, 운영모드, 메시지 인증코드, 키 유도 함수, 스트림암호 등이 이 부류에 속하는 암호기술이며, 이에 더해 키가 필요하지 않은 해시함수, 난수발생기, 확장 출력 함수 등도 대칭 키 암호에 포함할 수 있다. 이 문서에서는 대칭 키 암호를 유형별로 소개한다.

#### ❶ 블록암호

블록암호(block cipher)는 비밀 키를 이용하여 정해진 블록 길이(예 : 64비트, 128비트)의 평문을 암호화하는 대칭 키 암호기술이다. 암호화와 복호화에 같은 키를 사용하며, 높은 동작 속도와 구현의 편의성으로 인해 국가 · 공공 · 민간의 다양한 정보시스템에서 가장 널리 활용되는 암호기술 중 하나이다. 블록암호 알고리즘은 고정 길이의 한 블록 데이터 암호화만 정의하므로, CBC, CTR, GCM 등의 운영모드(modes of operation)와 결합하여야 임의 길이의 데이터 암호화에 사용할 수 있다.

**[그림 2] 블록암호 개념도**




KCMVP 검증대상 블록암호 알고리즘은 SEED, ARIA, HIGHT, LEA, AES이며, 이들 알고리즘의 명세는 국가 표준 또는 국제 표준으로 제정되어 있다. 따라서 특정 블록암호를 사용할 때는 해당 표준에 명시된 블록 길이, 키 길이, 라운드 구조, 키 스케줄 및 암·복호화 절차 등을 준수해야 한다.

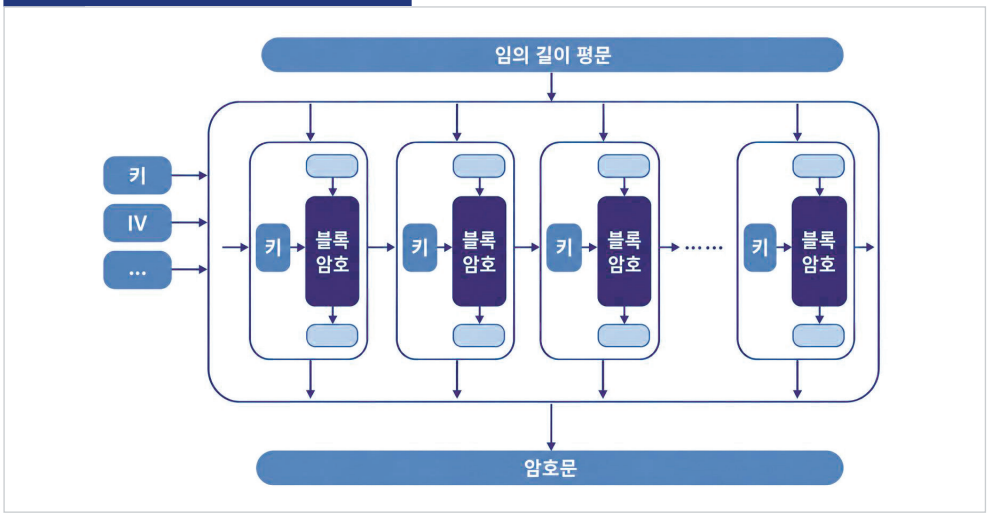
KCMVP 검증대상 블록암호 알고리즘은 [표 37]의 참조 표준에서 그 명세를 확인할 수 있다.

**[표 37] KCMVP 검증대상 블록암호 알고리즘 표준 목록**

| 알고리즘 | 참조 표준 |
|---|---|
| SEED | • [KS X ISO/IEC 18033-3] 정보기술 – 보안기술 – 암호 알고리즘 – 제3부 : 블록 암호 |
| ARIA | • [KS X 1213-1] 정보기술 – 보안기술 – 128비트 블록 암호 알고리즘 ARIA – 제1부 : 일반 |
| HIGHT | • [KS X ISO/IEC 18033-3] 정보기술 – 보안기술 – 암호 알고리즘 – 제3부 : 블록 암호 |
| LEA | • [KS X ISO/IEC 29192-2] 정보보안 – 경량 암호 – 제2부 : 블록 암호 |
| AES | • [KS X ISO/IEC 18033-3] 정보기술 – 보안기술 – 암호 알고리즘 – 제3부 : 블록 암호 |

블록암호 운영모드는 블록암호 알고리즘으로 임의 길이의 데이터를 안전하게 암호화하는 기술이다. 같은 블록암호를 사용하여도 운영모드에 따라 암호화 절차, 오류 전파 특성, 병렬 처리 가능 여부, 인증 기능 제공 여부 등이 달라진다. 따라서 암호화 기능의 실제 안전성은 운영모드의 선택에 크게 영향을 받는다고 볼 수 있다.

**[그림 3] 블록암호 운영모드 개념도**




국가·공공 정보시스템은 안전성이 검증되고 표준화된 운영모드를 적용하여야 하며, 따라서 KCMVP는 운영모드의 표준 적합 구현 여부를 중요하게 확인한다.

KCMVP 검증대상 블록암호 운영모드는 [표 38]의 참조 표준에서 그 명세를 확인할 수 있다.

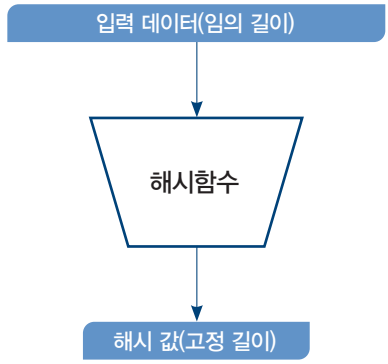
**[표 38] KCMVP 검증대상 블록암호 운영모드 표준 목록**

| 알고리즘 | 참조 표준 |
|---|---|
| ECB, CBC, CFB, OFB, CTR | • [KS X ISO/IEC 10116] 정보기술 – 보안기술 – n비트 블록 암호 운영 모드<br>• [KS X 3254] n비트 블록 암호 운영 모드 – 제1부 : 일반 |
| CCM, GCM | • [KS X ISO/IEC 19772] 정보기술 – 보안기술 – 인증된 암호화<br>• [KS X 3254] n비트 블록 암호 운영 모드 – 제1부 : 일반 |

## ❷ 해시함수

해시함수(hash function)는 임의 길이의 입력 데이터를 고정 길이 해시값으로 변환하는 암호기술이다. 해시함수는 데이터의 무결성을 보호하여 전자서명, 메시지 인증코드 등 다양한 암호기술의 설계 요소로 사용된다. 암호학적 해시함수는 해시값으로부터 입력값을 역산하기 어려운 역상 저항성(preimage resistance)과 서로 다른 입력이 같은 해시값을 갖는 쌍을 찾기 어려운 충돌 저항성(collision resistance)을 만족해야 한다.

**[그림 4] 해시함수 개념도**




KCMVP 검증대상 해시함수 알고리즘은 [표 39]의 참조 표준에서 그 명세를 확인할 수 있다.

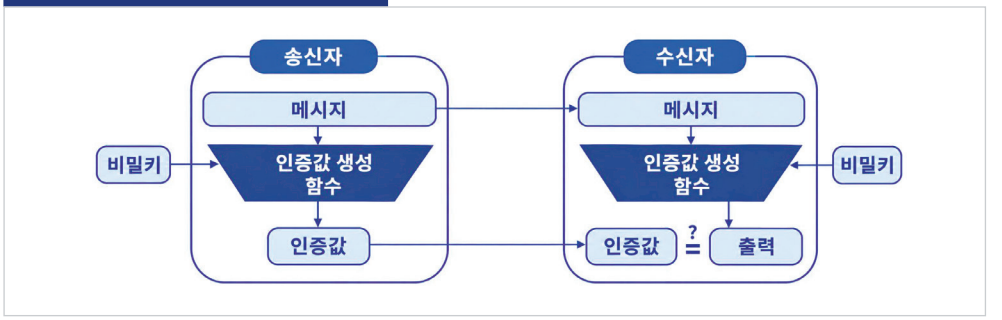
**[표 39] KCMVP 검증대상 해시함수 알고리즘 표준 목록**

| 알고리즘 | 참조 표준 |
|---|---|
| SHA2-224/256/384/512 | • [KS X ISO/IEC 10118-3] 정보기술 – 보안기술 – 해시함수 – 제3부 : 전용 해시 함수 |
| SHA3-224/256/384/512 | |
| LSH-224/256/384/512/ 512-224/512-256 | • [KS X 3262] 해시 함수 LSH |

## ❸ 메시지 인증코드

메시지 인증코드(message authentication code, MAC)는 송신자와 수신자가 공유한 비밀 키를 이용하여 메시지에 대한 인증값을 생성하고 검증함으로써, 데이터의 무결성과 송신자 인증을 동시에 제공하는 암호기술이다. 일반적으로 해시함수나 블록암호에 기반하여 설계하며, 비밀 키를 알고 있는 참여자만이 올바른 인증값을 생성하거나 검증할 수 있다.

**[그림 5] 메시지 인증코드 개념도**




KCMVP 검증대상 메시지 인증코드 알고리즘은 [표 40]의 참조 표준에서 그 명세를 확인할 수 있다.

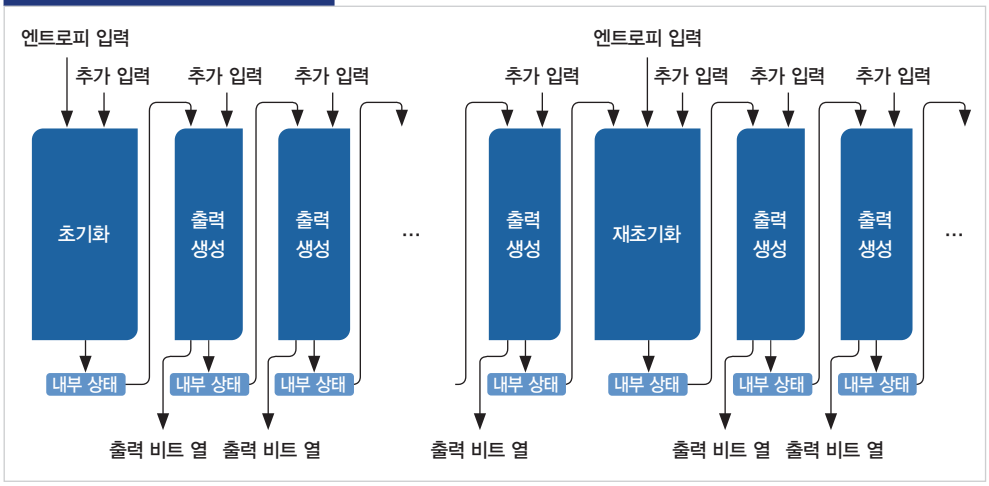
**[표 40] KCMVP 검증대상 메시지 인증코드 알고리즘 표준 목록**

| 알고리즘 | 참조 표준 |
|---|---|
| HMAC | • [KS X ISO/IEC 9797-2] 정보 보안 – 메시지 인증 코드 – 제2부 : 전용 해시 함수를 이용한 메커니즘 |
| CMAC | • [KS X 3254] n비트 블록 암호 운영 모드 – 제1부 : 일반 |
| GMAC | • [KS X 3254] n비트 블록 암호 운영 모드 – 제1부 : 일반 |

## ❹ 난수발생기

난수발생기(random number generator, RNG)는 암호 키, 초기화 벡터(IV), 논스(nonce), 인증토큰 등 암호시스템에 필요한 값을 생성하는 데 주로 사용하는 암호기술이다. 난수발생기의 출력은 통계적으로 균일하여야 하고, 입력과 내부상태를 알지 못하는 공격자는 예측할 수 없어야 한다. 난수발생기는 물리적 잡음을 정제하여 난수를 생성하는 실난수발생기(true random number generator, TRNG)와 결정론적 알고리즘에 엔트로피 입력을 주입하여 난수를 생성하는 의사난수발생기(pseudo-random number generator, PRNG)로 나눌 수 있다.

**[그림 6] 난수발생기 개념도**




KCMVP는 의사난수발생기 중에서도 무작위의 이진수열을 생성하는 DRBG(deterministic random bit generator)를 검증대상으로 하고 있으며, [표 41]의 참조 표준에서 그 명세를 확인할 수 있다.

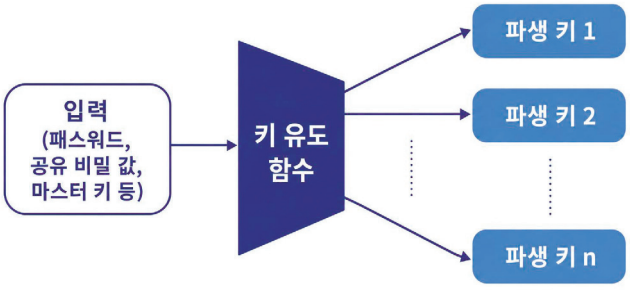
[표 41] KCMVP 검증대상 난수발생기(PRNG) 알고리즘 표준 목록

| 알고리즘 | 참조 표준 |
|---|---|
| CTR_DRBG,<br>HASH_DRBG,<br>HMAC_DRBG | • [KS X ISO/IEC 18031] 정보기술 – 보안기술 – 난수발생기 |

## ⑤ 키 유도 함수

키 유도 함수(key derivation function, KDF)는 비밀번호, 공유 비밀 값, 마스터키 등 제한된 입력으로부터 암호 키를 안전하게 생성하거나 여러 개의 파생키(derived key)를 생성하기 위해 사용하는 알고리즘이다. 키 유도 함수는 입력이 일부 노출되거나 난수성이 약한 경우에도 공격자가 키를 추측하기 어렵게 만들기 위해 입력의 특성이나 보안 요구사항에 따라 난수성 추출, 반복 연산, 솔트(salt) 및 컨텍스트 정보 결합 등의 방법을 사용하기도 한다.

[그림 7] 키 유도 함수 개념도




KCMVP 검증대상 키 유도 함수는 [표 42]의 참조 표준에서 그 명세를 확인할 수 있다.

[표 42] KCMVP 검증대상 키 유도 함수 표준 목록

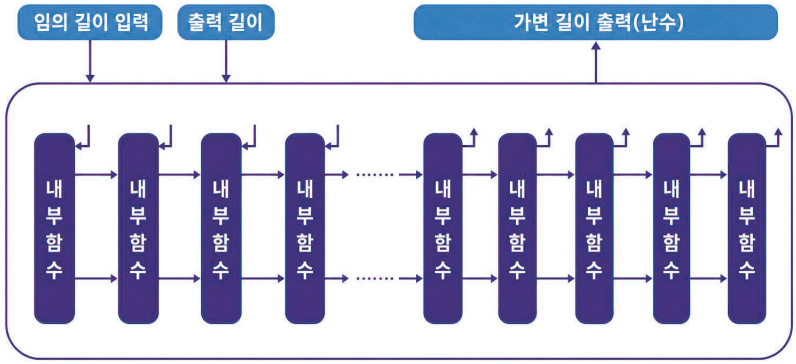
| 알고리즘 | 참조 표준 |
|---|---|
| KBKDF | • [ISO/IEC 11770-6] Information technology – Security techniques – Key management – Part 6 : Key derivation |
| PBKDF | • [TTAK.KO-12.0334] 패스워드 기반 키 유도 함수 |

## ⑥ 확장 출력 함수

확장 출력 함수(extendable-output function, XOF)는 임의 길이의 입력 데이터를 원하는 길이의 출력으로 변환하는 함수이다. 이는 출력 길이가 고정인 해시함수를 일반화한 개념으로, 해시함수의 역상 저항성과 같은 개념인 단방향성(one-wayness)과 충돌 저항성을 가져야 한다.

확장 출력 함수는 주로 양자내성암호의 내부 함수로 사용되면서 중요도가 높아진 기술이다. ISO/IEC에서는 기존 해시함수 표준의 정보 제공용(informative) 부속서로 확장 출력 함수를 명시하고 있다.

[그림 8] 확장 출력 함수 개념도




국내외에서 자주 사용하는 표준 확장 출력 함수 알고리즘은 [표 43]과 같다.

[표 43] 확장 출력 함수 알고리즘 표준 목록

| 알고리즘 | 참조 표준 |
|---|---|
| SHAKE128<br>SHAKE256 | • [ISO/IEC 10118-3] IT Security techniques – Hash-functions – Part 3 : Dedicated hash-functions |

## 제2절 비대칭 키 암호

비대칭 키 암호(asymmetric key cryptography)는 데이터를 암호학적으로 보호하고 처리하는 데 서로 다른 키를 사용하는 암호기술을 말한다. 공개 키 암호화와 전자서명이 대표적인 비대칭 키 암호기술이다. 공개 키 암호화와 전자서명은 두 개의 키를 사용하며, 그중 하나는 공개하여 데이터 암호화 또는 전자서명 검증에 사용하고, 나머지 하나는 비밀로 유지하며 암호문의 복호화 또는 전자서명 생성에 사용한다. 이 절에서는 비대칭 키 암호를 공개 키 암호화, 전자서명, 키 설정의 세 가지로 구분하여 소개한다. 전자서명은 기존 전자서명과 양자내성 전자서명으로, 키 설정은 키 합의와 키 캡슐화 메커니즘으로 나누어 다룬다.

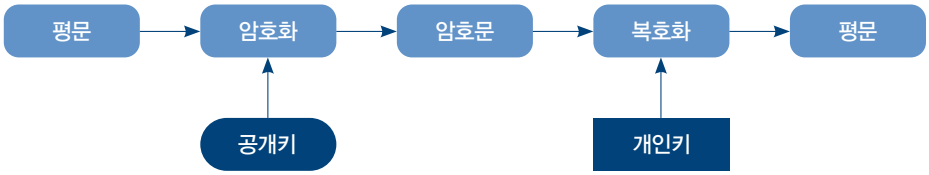
정수의 인수분해 문제나 유한체·타원곡선 상의 이산대수 문제의 어려움에 안전성을 기반하여 설계된 비대칭 키 암호는 양자컴퓨터가 충분히 발전하면 기반 문제가 쉽게 풀려 그 안전성을 유지하기 어렵다. 반면 양자내성암호는 양자컴퓨터로도 다항식 시간에 푸는 방법이 아직 알려지지 않은 새로운 수학적 난제(격자, 오류정정부호, 다변수 다항식 관련 문제 등)에 기반하거나 대칭 키 암호기술을 활용하여 설계한 비대칭 키 암호로, 양자내성 전자서명과 키 캡슐화 메커니즘이 이에 해당한다.

공개 키 암호화와 기존 전자서명, 키 합의는 현재 KCMVP 검증대상이며, 양자내성 전자서명과 양자내성 키 캡슐화 메커니즘에 대해서는 향후 검증 대상 추가를 검토하고 있다.

## ❶ 공개 키 암호화

공개 키 암호화(public key encryption)는 공개 키를 이용하여 누구나 메시지를 암호화할 수 있지만, 개인 키를 가진 사용자만 메시지를 복호화할 수 있는 데이터 암호화 기술이다.

[그림 9] 공개 키 암호화 개념도




KCMVP에서는 정수의 소인수분해 문제에 기반한 공개 키 암호화 알고리즘을 검증 대상으로 하고 있으며, [표 44]의 참조 표준에서 그 명세를 확인할 수 있다.

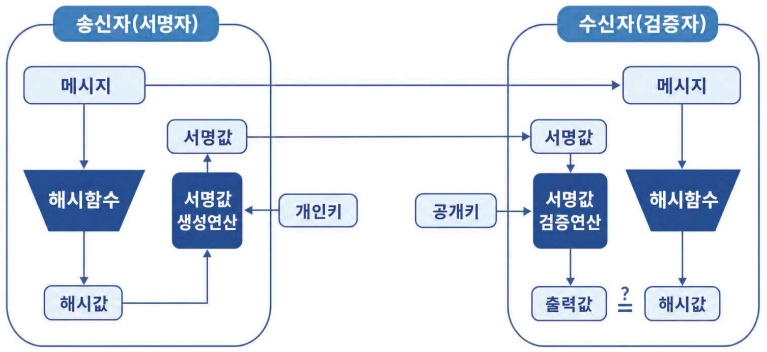
[표 44] KCMVP 검증대상 공개 키 암호화 알고리즘 표준 목록

| 알고리즘 | 참조 표준 |
|---|---|
| RSAES | • [KS X ISO/IEC 18033-2] 정보기술 – 보안기술 – 암호 알고리즘 – 제2부 : 비대칭형 암호 |

## ❷ 전자서명

전자서명(digital signature)은 서명자가 개인 키를 이용하여 서명값을 생성하면, 누구나 그 개인 키에 대응하는 공개 키로 해당 서명의 진위를 확인할 수 있는 비대칭 키 암호기술이다. 전자서명을 통하여 데이터의 무결성과 서명자의 신원을 확인할 수 있으며, 동시에 서명에 대한 부인방지(non-repudiation) 기능을 제공할 수 있다.

**[그림 10] 전자서명 개념도**




기존 전자서명은 현재 KCMVP 검증대상이므로 검증대상 알고리즘을 중심으로 정리하였고, 양자내성 전자서명은 아직 검증대상에 포함되지 않아 국내외에서 표준화가 완료되었거나 진행 중인 주요 알고리즘을 함께 정리하였다. 각 알고리즘의 명세는 [표 45], [표 46]의 참조 표준에서 확인할 수 있다.

**[표 45] KCMVP 검증대상 기존 전자서명 알고리즘 표준 목록**

| 알고리즘 | 참조 표준 |
|---|---|
| RSASSA | • [KS X ISO/IEC 14888-2] 정보기술 – 보안기술 – 부가형 디지털 서명 – 제2부 : 정수 인수분해 기반 메커니즘 |
| KCDSA, ECDSA, EC-KCDSA | • [KS X ISO/IEC 14888-3] 정보기술 – 보안기술 – 부가형 디지털 서명 – 제3부 : 이산대수 기반 메커니즘 |

**[표 46] 주요 양자내성 전자서명 알고리즘 예시**

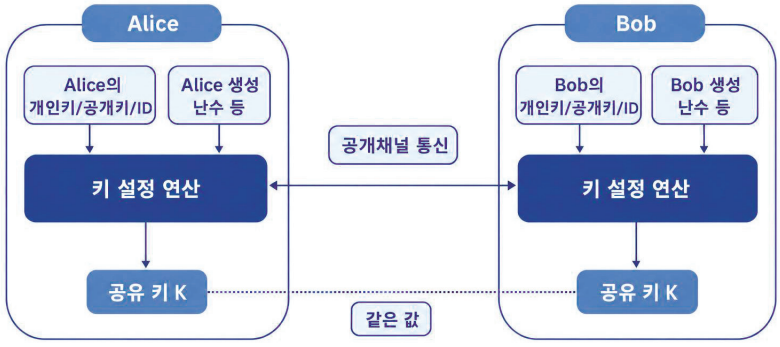
| 알고리즘 | 참조 표준 |
|---|---|
| ML-DSA | • [NIST FIPS 204] Module-Lattice-Based Digital Signature Standard |
| SLH-DSA | • [NIST FIPS 205] Stateless Hash-Based Digital Signature Standard |
| FN-DSA (Falcon) | • [NIST FIPS 206] FN-DSA (Falcon)(표준화 확정, 초안 발간 예정) |

| 알고리즘 | 참조 표준 |
|---|---|
| XMSS<br>LMS | • [ISO/IEC 14888-4] Information security – Digital signatures with appendix – Part 4 : Stateful hash-based mechanisms |
| AIMer | • KpqC Competition : KpqC Algorithms (KS 표준화 추진 중) |
| HAETAE | • KpqC Competition : KpqC Algorithms (KS 표준화 추진 중) |

## ❸ 키 설정

키 설정(key establishment)은 암호 통신을 하려는 모든 참여자가 같은 키를 안전하게 생성하거나 공유하기 위한 절차를 정의한 것으로, 보안 네트워크(TLS, VPN 등) 구축에 필수적인 암호기술이다.

[그림 11] 키 설정 개념도



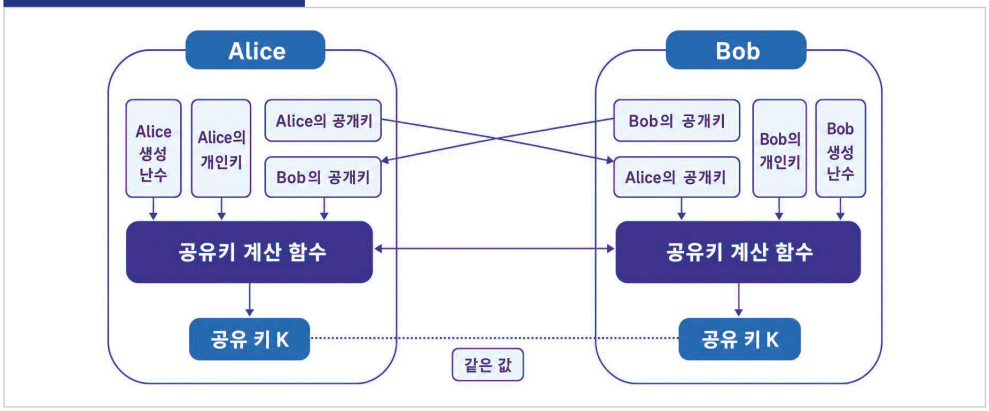

키 합의는 현재 KCMVP 검증대상이므로 검증대상 알고리즘을 중심으로 정리하였고, KEM은 아직 검증대상에 포함되지 않아 국내외에서 표준화가 완료되었거나 진행 중인 주요 알고리즘을 함께 정리하였다.

### 가. 키 합의

키 합의(key agreement)는 사전에 비밀을 공유하지 않은 참여자들이 공개

정보를 교환하는 것만으로 같은 키를 공유할 수 있게 하며, 공격자가 그 교환 과정에서 공개된 값을 획득하더라도 공유된 키를 알아내기 어렵게 설계한다.

**[그림 12] 키 합의 개념도**




KCMVP는 키 설정 알고리즘으로 키 합의만을 검증대상으로 한다. [표 47]의 참조 표준에서 그 명세를 확인할 수 있다.

**[표 47] KCMVP 검증대상 키 설정 알고리즘 표준 목록**

| 알고리즘 | 참조 표준 |
|---|---|
| DH(Diffie–Hellman), ECDH(Elliptic Curve Diffie–Hellman) | • [KS X ISO/IEC 11770–3] 정보기술 – 보안기술 – 키 관리 – 제3부 : 비대칭 기법을 이용한 메커니즘 |

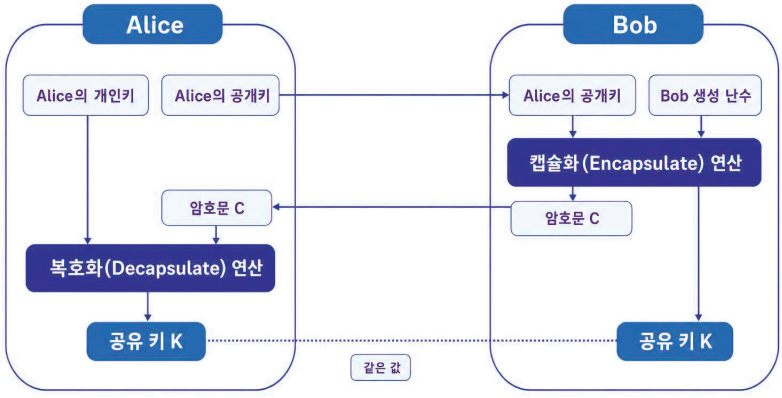
### 나. 키 캡슐화 메커니즘(KEM)

키 캡슐화 메커니즘(이하 KEM)은 암호 통신을 하려는 모든 참여자가 공개키 암호화를 사용하여 같은 비밀을 안전하게 공유하는 암호기술이다. 각 개체는 KEM을 통해 공유한 비밀 값으로 대칭 키 암호화에 사용하는 키를 생성하여 암호 통신을 진행하는 것이 일반적이다.

KEM의 대략적인 동작 과정은 다음과 같다. 한쪽 사용자는 랜덤한 메시지를

상대방의 공개 키로 암호화한 후 전송하고, 그 메시지와 암호문으로 비밀 값을 만든다. 반대쪽 사용자는 전송받은 암호문과 그 암호문을 자신의 개인 키로 복호화하여 얻은 메시지를 이용하여 같은 비밀 값을 얻는다. 마지막으로 양측은 얻어진 비밀 값을 키 유도 함수에 입력하여 같은 대칭 키를 생성한다.

**[그림 13] KEM 개념도**




KCMVP는 아직 KEM을 검증대상에 포함하지 않은 상태이며, 향후에는 양자내성 KEM을 검증대상 암호알고리즘에 포함할 예정이다. 국내외에서 안전성을 인정받아 표준화가 완료되었거나, 진행 중인 알고리즘은 [표 48]과 같다.

**[표 48] 주요 양자내성 KEM 알고리즘 예시**

| 알고리즘 | 참조 문헌 |
|---|---|
| ML-KEM | • [NIST FIPS 203] Module-Lattice-Based Key-Encapsulation Mechanism Standard |
| HQC | • [NIST FIPS 207] HQC-KEM (표준화 확정, 초안 발간 예정) |
| Classic McEliece | • [ISO/IEC 18033-2 : Amendment 2] Information technology – Security techniques – Encryption algorithms – Part 2 : Asymmetric ciphers |
| FrodoKEM | • [ISO/IEC 18033-2 : Amendment 2] Information technology – Security techniques – Encryption algorithms – Part 2 : Asymmetric ciphers |

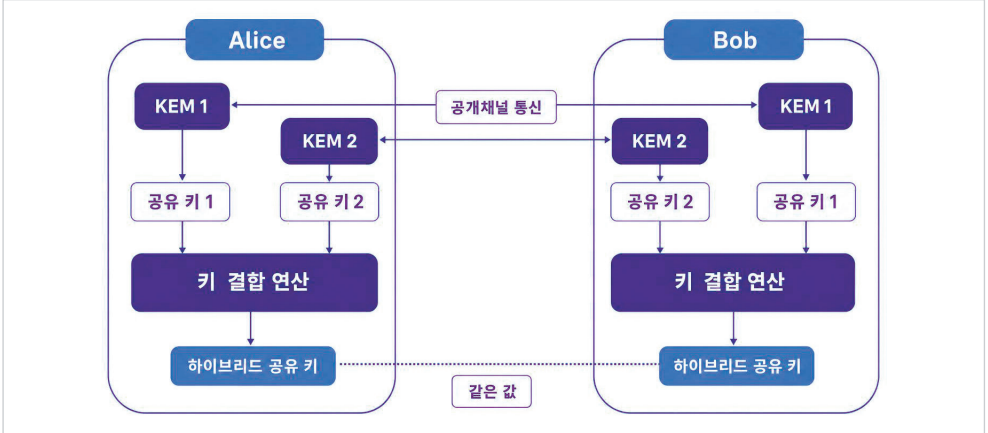
| 알고리즘 | 참조 문헌 |
|---|---|
| NTRU | • NIST PQC Standardization Process; Round 3 Finalists<br>• ISO/IEC 29192-4 : 2013/Amd 2 part 4(ISO/IEC 표준화 진행 중) |
| NTRU+ | • KpqC Competition : KpqC Algorithms(KS 표준화 진행 중) |
| SMAUG-T | • KpqC Competition : KpqC Algorithms(KS 표준화 진행 중) |

## ❹ 하이브리드

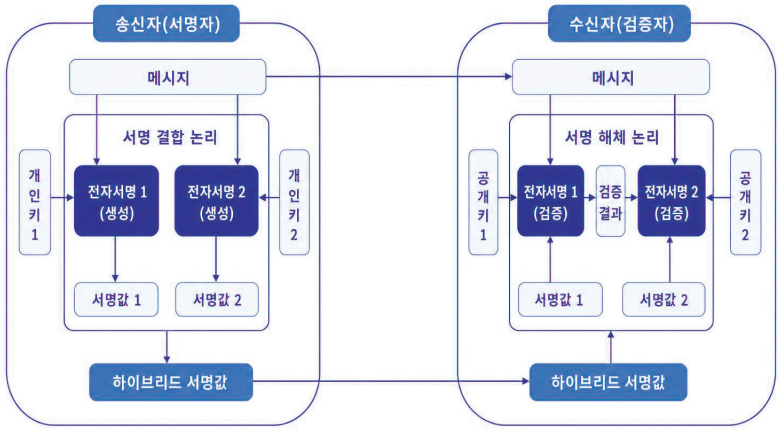
하이브리드는 둘 이상의 비대칭 키 암호 알고리즘을 함께 사용하여 정보를 보호하는 방식을 의미한다. 하이브리드는 함께 사용하는 알고리즘 중 일부가 취약해지더라도 전체 기능의 안전성이 저하되지 않도록 하는 목적으로 사용한다. 그러므로 보안 강도가 대등한 알고리즘의 결합을 원칙으로 하며, 하나의 알고리즘을 공격하여 얻은 정보로 다른 알고리즘을 쉽게 무력화할 수 없도록 설계하여야 한다.

하이브리드는 비대칭 키 암호기술 중 전자서명과 키 설정을 대상으로 기술개발 및 표준화가 진행되고 있다. 하이브리드는 결합하는 알고리즘의 종류에 따라, 기존 비대칭 키 암호와 양자내성암호를 결합하는 PQ/T 하이브리드와 서로 다른 양자내성암호를 결합하는 PQ/PQ 하이브리드로 구분할 수 있다.

[그림 14] 하이브리드 KEM 개념도



**[그림 15] 하이브리드 전자서명 개념도**




하이브리드 방식은 IETF를 중심으로 표준화가 논의 중이며, 표준화되었거나 현재 표준화가 진행 중인 기술은 [표 49]와 같다.

**[표 49] 표준화가 진행 중인 하이브리드 방식**

| 종류 | 참조 문헌 |
|---|---|
| 키 설정 | • [draft-irtf-cfrg-concrete-hybrid-kems] Concrete Hybrid PQ/T Key Encapsulation Mechanisms<br>• [draft-irtf-cfrg-hybrid-kems] Hybrid PQ/T Key Encapsulation Mechanisms<br>• [draft-connolly-cfrg-xwing-kem] X-Wing : general-purpose hybrid post-quantum KEM |
| 전자서명 | • [RFC 9955] Hybrid Signature Spectrums<br>• [draft-prabel-cfrg-suf-hybrid-sigs] Hybrid Digital Signatures with Strong Unforgeability |

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



# 주요 용어 및 약어

# 주요 용어 및 약어

## 1. 용어의 정의

### | 개인 키

비대칭 키 암호를 사용하는 한 개체가 소유한 키 쌍 중 공개하지 않는 키. 공개 키 암호화에서는 복호화 과정에, 전자서명에서는 서명 생성 과정에 사용한다.

### | 공개 키

비대칭 키 암호를 사용하는 한 개체가 소유한 키 쌍 중 공개하는 키. 공개 키 암호화에서는 암호화 과정에, 전자서명에서는 서명 검증 과정에 사용한다.

### | 공격 복잡도

공격자가 공격을 성공시키기 위해 수행해야 하는 연산 또는 자원의 양을 나타내며, 일반적으로 비트 단위의 보안 강도로 표현된다.

### | 기밀성

정당하지 않은 사용자나 시스템에 정보가 노출되지 않게 하는 특성. 기밀성의 보장을 위하여 암호화(encryption)가 사용된다.

### | 대칭 키 암호

데이터의 암호학적 보호와 처리에 같은 키를 사용하는 암호기술을 말한다. 비대칭 키 암호에 비해 동작 속도가 빠르지만 송수신자 간에 안전한 사전 키 분배가 필요하다.

### | 무결성

의도하지 않은 요인에 의해 데이터가 변경되거나 손상되지 않았다는 것을 보장하는 특성. 무결성의 보장을 위하여 해시함수, 메시지 인증코드, 전자서명 등이 사용된다.

### | 복호화

암호화(encryption)의 역과정으로, 암호 알고리즘과 키를 이용하여 암호문을 평문으로 바꾸는 과정.

### | 부인방지

메시지의 송수신이나 교환 또는 통신이나 처리가 실행된 사후에 그 사실을 증명함으로써 행위 사실을 부인하지 못하게 막음

### | 비대칭 키 암호

데이터의 암호학적 보호와 처리에 서로 다른 키를 사용하는 암호기술. 두 키중 하나는 공개하므로 공개 키 암호라고도 부른다. 안전한 사전 키 분배가 필요하지 않으며, 일반적으로 동작 속도가 대칭 키 암호에 비해 느리다.

### | 비밀 키

대칭 키 암호를 사용하기 위하여 정당하게 참여한 개체들만 공유하는 키

### | 소인수분해 문제

양의 정수의 소인수를 찾는 문제. 두 큰 소수의 곱으로 만들어진 합성수의 소인수분해는 매우 어려워 RSA 공개 키 암호의 기반 문제로 사용된다.

### | 실난수발생기

비결정론적인 물리적 현상을 이용하여 예측 불가능한 난수를 생성하는 장치

### | 암호모듈 검증제도

「사이버안보 업무규정」 제9조와 「전자정부 시행령」 제69조 등에 따라 국가·공공기관에서 도입하는 암호모듈의 안전성과 구현 적합성을 검증하는 제도

### | 암호화

암호 알고리즘과 키를 이용하여 평문을 암호문으로 바꾸는 과정. 복호화(decryption)의 역과정

### | 양자내성암호(PQC, Post-Quantum Cryptography)

RSA, ECC 등 기존의 공개 키 암호와 달리 양자 컴퓨터로도 해결이 어렵다고 알려진 수학적 난제에 안전성을 의존하여 설계된 비대칭 키 암호. 주로 격자, 오류정정부호, 다변수 다항식 분야의 난제를 사용함.

### | 양자컴퓨터

얽힘이나 중첩과 같은 양자역학 현상을 이용하여 연산을 수행하는 컴퓨터. 기존 컴퓨터로는 해결하기 어려운 문제를 쉽게 해결할 수 있는 알고리즘의 동작이 가능하여 암호의 해독에 사용될 잠재력이 있다.

### | 엔트로피

어떤 변수가 가진 정보의 양을 나타내는 척도. 같은 크기의 변수라도 엔트로피가 높을수록 변수가 가질 수 있는 값의 종류가 많아(정보량이 적음) 예측이 어렵고, 엔트로피가 낮을수록 변수가 가질 수 있는 값의 종류가 적어(정보량이 많음) 쉽게 예측이 가능하다.

### | 역상 저항성

주어진 출력에 대해 그 출력을 생성하는 입력을 찾는 것이 계산상 어려워야 한다는 특성(일방향성)이며, 암호학적 해시함수가 반드시 갖추어야 할 요건 중 하나이다.

### | 오류정정부호

원래 데이터에 여분의 정보를 추가하여 데이터의 전송 또는 저장 과정에서 발생하는 오류를 탐지하거나 정정할 수 있도록 하는 기술

### | 유한체

원소의 개수가 유한한 체. 체란 덧셈에 대하여 군을 이루고, 그 군에서 덧셈의 항등원을 제외한 집합이 곱셈에 대하여 군을 이루는 집합을 말한다.

### | 의사난수발생기

결정론적 알고리즘을 이용하여 난수를 생성하는 기술. 의사난수발생기의 출력은 초기 상태를 알면 같은 난수를 생성할 수 있으므로 실난수와 구별하여 의사난수라고 부른다.

### | 이산대수 문제

원소의 개수가 유한한 순환군에서 어떤 원소의 이산대수를 구하는 문제. 덧셈 군에서는 정수배의 역연산, 곱셈 군에서는 거듭제곱의 역연산을 수행하여야 해결할 수 있으며, 이들 문제는 매우 어려워 ECC 등 공개 키 암호의 기반 문제로 사용된다.

### | 인증

전송 또는 저장된 데이터의 출처나 시스템과 상호 작용하는 개체의 신원을 보증하기 위한 절차

### | 인증암호화

데이터를 암호화하면서 암호문과 인증값을 같이 생성하는 기술. 이를 통해 기밀성, 무결성, 출처 인증을 동시에 제공한다.

### | 충돌 저항성

같은 출력을 생성하는 서로 다른 두 입력을 찾는 것이 계산상 어려워야 한다는 특성이며, 암호학적 해시함수가 반드시 갖추어야 할 요건 중 하나이다.

### | 키 합의

키 설정의 한 종류로, 키 설정에 참여한 어떠한 개체도 다른 참여 개체의 도움 없이 독립적으로 공유키를 계산할 수 없도록 설계된 방식

## 2. 약어

| | |
|---|---|
| CBC | Cipher Block Chaining |
| CCM | Counter with CBC-MAC |
| CFB | Cipher Feedback |
| CRQC | Cryptographically Relevant Quantum Computer |
| CTR | Counter |
| DRBG | Deterministic Random Bit Generator |
| DSA | Digital Signature Algorithm |
| ECB | Electronic Codebook |
| ECC | Elliptic Curve Cryptography |
| ECCG | European Cybersecurity Certification Group |
| (EC)DH | (Elliptic Curve) Diffie-Hellman |
| (EC)DLP | (Elliptic Curve) Discrete Logarithm Problem |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EC-KCDSA | Elliptic Curve Korean Certificate-based Digital Signature Algorithm |
| ENISA | European Union Agency for Cybersecurity |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| FIPS | Federal Information Processing Standard |
| GCM | Galois/Counter Mode |
| GNFS | General Number Field Sieve |
| IEC | International Electrotechnical Commission |

| | |
|---|---|
| **IETF** | Internet Engineering Task Force |
| **ISO** | International Organization for Standardization |
| **IV** | Initialization Vector |
| **KBKDF** | Key Based Key Derivation Function |
| **KCMVP** | Korea Cryptographic Module Validation Program |
| **KDF** | Key Derivation Function |
| **KEM** | Key Encapsulation Mechanism |
| **KISA** | Korea Internet and Security Agency |
| **KS** | Korean Standard |
| **LWE** | Learning With Errors |
| **MAC** | Message Authentication Code |
| **NIS** | National Intelligence Service |
| **NIST** | National Institute of Standards and Technology |
| **NSR** | National Security Research Institute |
| **OFB** | Output Feedback |
| **PBKDF** | Password Based Key Derivation Function |
| **PQC** | Post-Quantum Cryptography |
| **PRNG** | Pseudo-Random Number Generator |
| **RFC** | Request For Comments |
| **SVP** | Shortest Vector Problem |
| **TLS** | Transport Layer Security |
| **VPN** | Virtual Private Network |
| **XOF** | Extendable Output Function |

# 국가 · 공공기관 **암호 안전성 기준**

CRYPTOGRAPHIC SECURITY GUIDELINE



# 참고 문헌

# 참고 문헌

1. 관계부처합동, “범국가 양자내성암호 전환 마스터플랜”, 2023.

2. 관계부처합동, “범국가 양자내성 암호체계 전환 종합 추진계획”, 2025.

3. 국가정보원, “국가·공공기관 암호 사용 기준”, 2009.

4. 국가정보원, 국가보안기술연구소, “암호모듈 구현안내서 Part 1 : 시험 및 구현 사례별 해설서”, 2025.

5. 국가정보원, 국가보안기술연구소, “암호모듈 구현안내서 Part 2 : 검증대상 암호알고리즘 구현안내서”, 2025.

6. 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2018.

7. KS X 1213-1, “정보기술 - 보안기술 - 128비트 블록 암호 알고리즘 ARIA - 제1부 : 일반”, 2024.

8. KS X 3254, “n비트 블록 암호 운영 모드 - 제1부 : 일반”, 2016.

9. KS X 3262, “해시 함수 LSH”, 2023.

10. KS X ISO/IEC, “9797-2 : 정보 보안 - 메시지 인증 코드 - 제2부 : 전용 해시 함수를 이용한 메커니즘”, 2024.

11. KS X ISO/IEC, “10116 : 정보기술 - 보안기술 - n비트 블록 암호 운영 모드”, 2021.

12. KS X ISO/IEC, “10118-3 : 정보기술 - 보안기술 - 해시 함수 - 제3부 : 전용 해시 함수”, 2023.

13. KS X ISO/IEC, “11770-3 : 정보기술 - 보안기술 - 키 관리 - 제3부 : 비대칭 기법을 이용한 메커니즘”, 2024.

14. KS X ISO/IEC, “14888-2 : 정보기술 – 보안기술 – 부가형 디지털 서명 – 제2부 : 정수 인수분해 기반 메커니즘”, 2021.

15. KS X ISO/IEC, “14888-3 : 정보기술 – 보안기술 – 부가형 디지털 서명 – 제3부 : 이산대수 기반 메커니즘”, 2021.

16. KS X ISO/IEC, “18031 : 정보기술 – 보안기술 – 난수발생기”, 2023.

17. KS X ISO/IEC, “18033-2 : 정보 기술 – 보안 기술 – 암호 알고리즘 – 제2부 : 비대칭형 암호”, 2022.

18. KS X ISO/IEC, “18033-3 : 정보기술 – 보안기술 – 암호 알고리즘 – 제3부 : 블록 암호”, 2023.

19. KS X ISO/IEC, “19772 : 정보기술 – 보안기술 – 인증된 암호화”, 2024.

20. KS X ISO/IEC, “29192-2 : 정보기술 – 보안기술 – 경량 암호기법 – 제2부 : 블록 암호”, 2024.

21. 한국정보통신기술협회, “TTAK.KO-12.0334 : 패스워드 기반 키 유도 함수 – 제1부 : 일반.”, 2018.

22. AIVD, CWI, TNO, “The PQC Migration Handbook. 2nd edn.”, 2024.

23. ANSSI, “ANSSI-PG-083, Version 3.00, Règles et recommandations concernant le choix et le dimensionnement des mècanismes cryptographiques”, 2026. (in French)

24. Biham, E., “New Types of Cryptanalytic Attacks Using Related Keys”, Journal of Cryptology 7, 1994.

25. Bindel, N., Hale, B., Connolly, D., Driscoll, F., “Hybrid Signature Spectrums”, IETF, 2026.

26. Biryukov, A., Khovratovich, D., “ Related-Key Cryptanalysis of the Full AES-192 and AES-256”, In, ASIACRYPT 2009. LNCS, vol. 5912. Springer, 2009.

27. Brassard, G., Hoyer, P., Tapp, A., “Quantum Cryptanalysis of Hash and Claw-Free Functions”, ACM SIGACT News 28, 1997.

28. BSI, “TR-02102-1 Version 2026-01: Cryptographic Mechanisms: Recommendations and Key Lengths”, 2026.

29. Buhler, J.P., Lenstra Jr., H.W., Pomerance, C., “Factoring integers with the number field sieve”, Lecture Notes in Mathematics, vol. 1554. Springer, 1993.

30. Castryck, W., Decru, T., “An Efficient Key Recovery Attack on SIDH”, In: EUROCRYPT 2023, 2023.

31. CCCS, “ITSM.40.001 : Roadmap for the migration to post-quantum cryptography for the Government of Canada”, 2025.

32. CCCS, “ITSP.40.111 Version 5: Cryptographic algorithms for UNCLASSIFIED, PROTECTED A and PROTECTED B information”, 2026.

33. CRYPTREC, “LS-0001-2022R2: List of Ciphers to be Referred to in Procurement for e-Government (CRYPTREC Cipher List)”, 2026. (in Japanese)

34. CRYPTREC, “LS-0003-2022R1: Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)”, 2023. (in Japanese)

35. ECCG, “Agreed Cryptographic Mechanisms. ENISA, Working Draft”, 2026.

36. Electronic Frontier Foundation, “Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design”, O’Reilly & Associates, 1998.

37. Gidney, C., “How to factor 2048 bit RSA integers with less than a million noisy qubits”, arXiv: 2505.15917, 2025.

38. Gidney, C., Eker?, M., “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5”, 2021.

39. Google Quantum AI, “Quantum Error Correction Below the Surface Code Threshold”, Nature, 2025.

40. Grover, L.K., “A fast quantum mechanical algorithm for database search”, In: STOC 1996, 1996.

41. Hemmert, T., Wiemers, A., “Distinguishing Goppa Codes Using Higher-Order Vanishing”, In : CRYPTO 2026, 2026.

42. ICBR, “Rijksbreed beleidskader cryptografie: Een raamwerk voor het opstellen van cryptografiebeleid”, BZK, Versie 1.0, 2025. (in Dutch)

43. Inter-ministerial Liaison Conference on the Use of Post-Quantum Cryptography (PQC) in Government Agencies, “Migration to Post-Quantum Cryptography (PQC) at Government Agencies, etc. (Interim Report)”, 2025. (in Japanese)

44. ISO/IEC, “10118-3: IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions”, 2018.

45. ISO/IEC, “11770-6: Information technology – Security techniques – Key management – Part 6: Key derivation”, 2016.

46. ISO/IEC, “14888-4: Information security – Digital signatures with appendix – Part 4 : Stateful hash-based mechanisms”, 2024.

47. ISO/IEC, “18033-2: Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers – Amendment 2”, 2026.

48. Microsoft Security Response Center, “Flame malware collision attack explained (Microsoft Security Advisory 2718704)”, 2012.

49. Mosca, M., “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?”, IEEE S&P 16, 2018.

50. Mosca, M., Piani, M., “Quantum Threat Timeline Report 2025”, Global Risk Institute, 2026.

51. NCSC-NL, “Transport Layer Security (TLS) Security guidelines. Version 2025-05”, 2025.

52. NCSC-UK, “Timelines for migration to post-quantum cryptography. Version 1.0”, 2025.

53. NCSC-UK, “Using TLS to protect data. Version 1.1”, 2025.

54. NIST, “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard”, 2024.

55. NIST, “FIPS 204: Module-Lattice-Based Digital Signature Standard”, 2024.

56. NIST, “SP 800-131A: Transitioning the Use of Cryptographic Algorithms and Key Lengths”, 2011.

57. NIST, “SP 800-131A Rev. 3: Initial Public Draft, Transitioning the Use of Cryptographic Algorithms and Key Lengths”, 2024.

58. Shor, P.W., “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Journal on Computing 26, 1997.

59. Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y., “The First Collision for Full SHA-1”, In: CRYPTO 2017. LNCS, vol. 10401. Springer, 2017.

60. TBS, “SPIN 2025-01: Migrating the Government of Canada to Post-Quantum Cryptography: Security Policy Implementation Notice”, 2025.

61. The White House, “Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks”, 2026.

62. Wang, X., Yin, Y.L., Yu, H., “Finding Collisions in the Full SHA-1”, In: CRYPTO 2005. LNCS, vol. 3621. Springer, 2005.

63. Wang, X., Yu, H., “How to Break MD5 and Other Hash Functions”, In: EUROCRYPT 2005. LNCS, vol. 3494. Springer, 2005.