

DIN SPEC 91444:2021-04 (E)

Definition of a quantum computer resistant encryption scheme; Text in English

Inhalt	Seite
Foreword	5
Introduction.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions.....	7
4 Symbols and abbreviations.....	8
5 Specification of KINDI-KEM — A post-quantum key encapsulation mechanism	11
5.1 General.....	11
5.2 Specification of KINDI-KEM — CPA-secure encryption	12
5.2.1 Description of key generation.....	12
5.2.2 Description of the encryption procedure	16
5.2.3 Description of the decryption procedure	20
5.3 Specification of KINDI-KEM – CCA-secure key encapsulation mechanism.....	23
5.3.1 Description of key generation.....	23
5.3.2 Description of the encapsulation procedure.....	23
5.3.3 Description of the decapsulation procedure	24
5.4 Number-theoretic transform (NTT)	24
5.5 Optimizations	25
5.5.1 General.....	25
5.5.2 Polynomial multiplication.....	25
5.5.3 Advanced Vector Extensions (AVX)	25
5.5.4 Modular reductions	26
5.5.5 Encoding and decoding.....	26
5.5.6 Secret key	26
5.6 Parameters and instantiations	26
5.6.1 Choice of parameter sets.....	26
5.6.2 SHAKE instantiation	27
5.6.3 Advanced Encryption Standard (AES) instantiation	27
6 Implementation security	28
6.1 General.....	28
6.2 Learnings from attacks on classical cryptography	28
6.3 Specific threats to lattice-based cryptography	29
7 Requirements for cryptosystems.....	29
7.1 General.....	29
7.2 Target of evaluation (TOE).....	30
7.3 Requirements	31
7.3.1 General description of the TOE.....	31
7.3.2 Determination of the TOE.....	31
7.3.3 Product lifecycle (installation, delivery, decommissioning).....	31
7.3.4 Architecture and design	31
7.3.5 Cryptography	31
7.3.6 Vulnerability management	31
7.3.7 Patch management	32
7.3.8 Change management	32
7.3.9 Incident management.....	32

7.3.10 Risk management.....	32
Annex A (informative) Security risk of quantum computing and counter measures.....	33
A.1 Security risk of quantum computing.....	33
A.1.1 Quantum computing differentiation from classical computing.....	33
A.1.2 Quantum computing impact on encryption schemes.....	34
A.2 Counter measures.....	34
A.2.1 General.....	34
A.2.2 Post-quantum cryptography.....	34
A.2.3 Quantum cryptography.....	34
A.2.4 Hybrid cryptography.....	35
A.3 Applications of post-quantum key encapsulation mechanisms.....	35
A.3.1 General.....	35
A.3.2 Key exchange and encryption.....	35
Bibliography.....	36

Tables

Table 1 — Key generation algorithm for CPA secure encryption.....	13
Table 2 — Subroutine to generate the NTT of the random matrix A.....	13
Table 3 — Subroutine to convert binary strings to integer representations.....	14
Table 4 — Subroutine to generate secret polynomials.....	15
Table 5 — Subroutine to convert polynomials into a binary string.....	16
Table 6 — Subroutine to convert an integer value into a binary string.....	16
Table 7 — Encryption routine.....	17
Table 8 — Auxiliary encryption subroutine.....	17
Table 9 — Subroutine to convert a bit string into a vector of polynomials.....	18
Table 10 — Subroutine to deterministically derive secrets from a random string.....	19
Table 11 — Subroutine to center the coefficients of polynomials around zero.....	19
Table 12 — Subroutine to compress a polynomial.....	20
Table 13 — Decryption routine.....	21
Table 14 — Subroutine to recover all secret values.....	21
Table 15 — Subroutine to decompress a polynomial.....	22
Table 16 — Subroutine to recover a binary polynomial from an input polynomial.....	22
Table 17 — Subroutine to convert centered coefficients into non-negative integers.....	22
Table 18 — Key generation algorithm for key encapsulation.....	23
Table 19 — Encapsulation algorithm.....	24

Table 20 — Decapsulation algorithm.....	24
Table 21 — Parameters.....	26
Table 22 — Sizes of keys and ciphertexts.....	27
Table A.1 — Performance differences between classical computers and quantum computers.....	33