

TCG Algorithm Registry

Version 2.0
July 28, 2025

Contact: admin@trustedcomputinggroup.org

TCG Published

DISCLAIMERS, NOTICES, AND LICENSE TERMS

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

DOCUMENT STYLE

Key Words

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document’s normative statements are to be interpreted as described in [RFC 2119: Key words for use in RFCs to Indicate Requirement Levels](#).

Statement Type

Please note an important distinction between different sections of text throughout this document. There are two distinctive kinds of text: *informative comments* and *normative statements*. Because most of the text in this specification will be of the kind *normative statements*, the authors have informally defined it as the default and, as such, have specifically called out text of the kind *informative comment*. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind *informative comment*, it can be considered a *normative statement*.

EXAMPLE:

Informative comment:

Reach out to admin@trustedcomputinggroup with any questions about this document.

Contents

1	Introduction	6
2	TCG_ALG_ID Values	7
3	TCG_ECC_CURVE Values	15
4	TCG_MLKEM_PARAMETER_SET Values	16
5	TCG_MLDSA_PARAMETER_SET Values	17
6	TCG_SLHDSA_PARAMETER_SET Values	18
7	Hash Algorithms Bit Field	19
	Appendices	20
A	Change History	21
B	Hash-Based Signature Parameters and Considerations	23
B.1	Introduction	23
B.2	NIST Parameter Sets	23
C	ECC Curve Parameters	25
C.1	Introduction	25
C.2	NIST_P192	25
C.3	NIST_P224	25
C.4	NIST_P256	26
C.5	NIST_P384	27
C.6	NIST_P521	27
C.7	BN_P256	28
C.8	BN_P638	29
C.9	SM2_P256	30
C.10	BP_P256_R1	31
C.11	BP_P384_R1	31
C.12	BP_P512_R1	32
C.13	CURVE_25519	33
C.14	CURVE_448	34
D	Hash Parameters	36
D.1	Introduction	36
D.2	SHA1	36
D.3	SHA256	36
D.4	SHA384	36
D.5	SHA512	36
D.6	SM3_256	37
D.7	SHA3_256	37
D.8	SHA3_384	37
D.9	SHA3_512	37
	References	38

List of Tables

1	Legend for TCG_ALG_ID Table	7
2	Definition of (UINT16) TCG_ALG_ID Constants	7
3	Definition of (UINT16) TCG_ECC_CURVE Constants	15
4	Definition of (UINT16) TCG_MLKEM_PARAMETER_SET Constants	16
5	Definition of (UINT16) TCG_MLDSA_PARAMETER_SET Constants	17
6	Definition of (UINT16) TCG_SLHDSA_PARAMETER_SET Constants	18
7	Definition of (UINT32) TPMA_HASH_ALGS Bits	19
8	Parameters for LMS and XMSS Approved in SP 800-208	23

1 Introduction

The Algorithm Registry lists each algorithm assigned an identifier, allowing it to be unambiguously defined and referenced by other TCG specifications. This document is a compendium of data related to the various algorithms used in specifications created by the Trusted Computing Group (TCG). The compendium of algorithm data is intended to ensure interoperability between devices built to be compliant with TCG specifications.

TCG as an organization does not perform cryptographic analysis of algorithms. The presence of an algorithm in the registry does not endorse its use by TCG for any specific use case or indicate an algorithm's acceptability for meeting any particular requirement set. The TCG endeavors to provide a variety of algorithms of varying strength for various commercial purposes. Ultimately, the TCG adds algorithms to its registry based on the needs of its membership.

Implementers or adopters of any solution using TCG specifications must carefully assess the appropriateness of any algorithms or TCG specification for satisfying their goals. In assessing algorithms, TCG recommends implementers and adopters diligently evaluate available information such as governmental, industrial, and academic research. Solutions involving cryptography are dependent on the solution architecture and on the properties of cryptographic algorithms supported. Over time, cryptographic algorithms can develop deficiencies for reasons like advances in cryptographic techniques or increased computing power. Solutions that support a diversity of algorithms can remain durable when subsets of supported algorithms wane in usefulness. Therefore, implementers intent on providing robust solutions are responsible for evaluating both algorithm appropriateness and diversity.

The TCG classifies algorithms listed in this registry according to the following labels:

- **TCG Standard** - The algorithm is mandatory in one or more TCG specifications that reference this registry. The TCG designates algorithms with this classification in accordance with its goals of promoting international standards and interoperability.
- **TCG Legacy** – The algorithm is assigned an identifier for compatibility or historical reasons and is unlikely to be referenced by future TCG specifications. The TCG designates an algorithm with this classification based on the goals of the organization to discontinue support for the algorithm and transition solutions to alternative algorithms. Stakeholders using solutions relying on algorithms classified as TCG Legacy are strongly recommended to reevaluate the algorithm's appropriateness based on the current state of the art.

Note:

Some TCG documents might continue to reference TCG Legacy algorithms in non-cryptographic contexts.

- **Assigned** – The algorithm is assigned an identifier, allowing it to be unambiguously defined and referenced by other TCG specifications, but is not designated as TCG Standard or TCG Legacy.

In terms of algorithm lifecycle in the registry, the TCG will initially assign algorithms to the Assigned classification. Some algorithms will be reclassified as TCG Standard if they become mandatory algorithms in TCG specifications. Eventually, algorithms are expected to transition to the TCG Legacy categorization.

2 TCG_ALG_ID Values

Table 2 is the list of algorithms to which the TCG has assigned an algorithm identifier along with its numeric identifier.

The values for TCG_ALG_ID are between 0x0001 and 0x7FFF.

Table 1: Legend for TCG_ALG_ID Table

Column Title	Comments
Algorithm Name	the mnemonic name assigned to the algorithm
Value	the numeric value assigned to the algorithm
C	(Classification) The allowed values are: A – Assigned S – TCG Standard L – TCG Legacy
Reference	the reference document that defines the algorithm
Comments	clarifying information

Note:

Previously published versions of this registry used the TPM_ prefix for values in Table 2 and Table 3. Other TCG documents might use the TPM_ prefix to refer to TCG_ values from this registry.

Table 2: Definition of (UINT16) TCG_ALG_ID Constants

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_RSA	0x0001	S	IETF RFC 8017 [1]	
TCG_ALG_TDES	0x0003	L	ISO/IEC 18033-3 [2]	
TCG_ALG_SHA1	0x0004	L	ISO/IEC 10118-3 [3]	
TCG_ALG_HMAC	0x0005	S	ISO/IEC 9797-2 [4]	
TCG_ALG_AES	0x0006	S	ISO/IEC 18033-3 [2]	
TCG_ALG_MGF1	0x0007	S	IEEE Std 1363™-2000 [5] IEEE Std 1363a™-2004 [6]	
TCG_ALG_KEYEDHASH	0x0008	S	TCG TPM 2.0 library specification [7]	an object type that may use XOR for encryption or an HMAC for signing and may also refer to a data object that is neither signing nor encrypting

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_XOR	0x000A	S	TCG TPM 2.0 library specification [7]	
TCG_ALG_SHA256	0x000B	S	ISO/IEC 10118-3 [3]	
TCG_ALG_SHA384	0x000C	S	ISO/IEC 10118-3 [3]	
TCG_ALG_SHA512	0x000D	A	ISO/IEC 10118-3 [3]	
TCG_ALG_SHA256_192	0x000E	A	NIST SP 800-208 [8]	the most significant (i.e., leftmost) 192 bits of the SHA-256 hash Note: This truncated hash is for use with LMS and XMSS. See Clause B.
TCG_ALG_NULL	0x0010	S	TCG TPM 2.0 library specification [7]	“Null” algorithm (i.e., none)
TCG_ALG_SM3_256	0x0012	A	ISO/IEC 10118-3:2018 [3]	
TCG_ALG_SM4	0x0013	A	GB/T 32907-2016 [9]	
TCG_ALG_RSASSA	0x0014	S	IETF RFC 8017 [1]	a signature algorithm defined in section 8.2 (RSASSA-PKCS1-v1_5)
TCG_ALG_RSAES	0x0015	S	IETF RFC 8017 [1]	a padding algorithm defined in section 7.2 (RSAES-PKCS1-v1_5)
TCG_ALG_RSAPSS	0x0016	S	IETF RFC 8017 [1]	a signature algorithm defined in section 8.1 (RSASSA-PSS)
TCG_ALG_OAEP	0x0017	S	IETF RFC 8017 [1]	a padding algorithm defined in section 7.1 (RSAES_OAEP)
TCG_ALG_ECDSA	0x0018	S	ISO/IEC 14888-3 [10]	signature algorithm using elliptic curve cryptography (ECC) (Non-deterministic ECDSA)
TCG_ALG_ECDH	0x0019	S	NIST SP 800-56A [11] IETF RFC 7748 [12]	secret sharing using ECC Based on context, this can be either One-Pass Diffie-Hellman, C(1, 1, ECC CDH) defined in 6.2.2.2, Full Unified Model C(2, 2, ECC CDH) defined in 6.1.1.2 of SP 800-56A, or X25519 defined in 5. of RFC 7748

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_ECDA	0x001A	S	TCG TPM 2.0 library specification [7]	elliptic-curve based, anonymous signing scheme
TCG_ALG_SM2	0x001B	A	GB/T 32918.1-2016 [13] GB/T 32918.2-2016 [14] GB/T 32918.3-2016 [15] GB/T 32918.4-2016 [16] GB/T 32918.5-2017 [17]	depending on context, either an elliptic-curve based signature algorithm, an encryption scheme, or a key exchange protocol
TCG_ALG_ECSCNORR	0x001C	S	TCG TPM 2.0 library specification [7]	elliptic-curve based Schnorr signature
TCG_ALG_ECMQV	0x001D	A	NIST SP 800-56A [11]	two-phase elliptic-curve key exchange – C(2, 2, ECC MQV) section 6.1.1.4
TCG_ALG_HKDF	0x001F	A	IETF RFC 5869 [18]	HMAC-based Extract-and-Expand Key Derivation Function
TCG_ALG_KDF1_SP800_56A	0x0020	S	NIST SP 800-56A [11]	concatenation key derivation function (approved alternative 1) section 5.8.1
TCG_ALG_KDF2	0x0021	A	IEEE Std 1363a-2004 [6]	key derivation function KDF2 section 13.2
TCG_ALG_KDF1_SP800_108	0x0022	S	NIST SP 800-108 [19]	Section 5.1 KDF in Counter Mode
TCG_ALG_ECC	0x0023	S	ISO/IEC 15946-1 [20]	prime field ECC
TCG_ALG_SYMCIPHER	0x0025	S	TCG TPM 2.0 library specification [7]	the object type for a symmetric block cipher
TCG_ALG_CAMELLIA	0x0026	A	ISO/IEC 18033-3 [2]	
TCG_ALG_SHA3_256	0x0027	A	ISO/IEC 10118-3 [2]	
TCG_ALG_SHA3_384	0x0028	A	ISO/IEC 10118-3 [2]	
TCG_ALG_SHA3_512	0x0029	A	ISO/IEC 10118-3 [2]	
TCG_ALG_SHAKE128	0x002A	A	ISO/IEC 10118-3 [2]	Extendable-output function providing up to 128 bits of collision and preimage resistance

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_SHAKE256	0x002B	A	ISO/IEC 10118-3 [2]	Extendable-output function providing up to 256 bits of collision and preimage resistance
TCG_ALG_SHAKE256_192	0x002C	A	NIST SP 800-208 [8]	the first 192 bits of SHAKE256 output
TCG_ALG_SHAKE256_256	0x002D	A	NIST SP 800-208 [8]	the first 256 bits of SHAKE256 output
TCG_ALG_SHAKE256_512	0x002E	A	IETF RFC 8032 [21]	the first 512 bits of SHAKE256 output
TCG_ALG_CMAC	0x003F	A	ISO/IEC 9797-1:2011 [22]	Block Cipher-based Message Authentication Code (CMAC) “Algorithm 5” in ISO/IEC 9797-1:2011
TCG_ALG_CTR	0x0040	A	ISO/IEC 10116 [23]	Counter mode
TCG_ALG_OFB	0x0041	A	ISO/IEC 10116 [23]	Output Feedback mode
TCG_ALG_CBC	0x0042	A	ISO/IEC 10116 [23]	Cipher Block Chaining mode
TCG_ALG_CFB	0x0043	S	ISO/IEC 10116 [23]	Cipher Feedback mode
TCG_ALG_ECB	0x0043	L	ISO/IEC 10116 [23]	Electronic Codebook mode Note: This mode is not recommended for use unless the key is frequently rotated, such as in video codecs.
TCG_ALG_CCM	0x0050	A	NIST SP 800-38C [24]	Counter with Cipher Block Chaining-Message Authentication Code
TCG_ALG_GCM	0x0051	A	NIST SP 800-38D [25]	Galois/Counter Mode
TCG_ALG_KW	0x0052	A	NIST SP 800-38F [26]	AES Key Wrap
TCG_ALG_KWP	0x0053	A	NIST SP 800-38F [26]	AES Key Wrap with Padding
TCG_ALG_EAX	0x0054	A	ISO/IEC 19772 [27]	Authenticated-Encryption Mode

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_EDDSA	0x0060	A	IETF RFC 8032 [21]	Edwards-curve Digital Signature Algorithm (PureEdDSA) Note: EdDSA requires Twisted Edwards curves
TCG_ALG_HASH_EDDSA	0x0061	A	IETF RFC 8032 [21]	Edwards-curve Digital Signature Algorithm (HashEdDSA) Note: EdDSA requires Twisted Edwards curves
TCG_ALG_RSASVE_KEM	0x0062	A	NIST SP 800-227 [28]	Key Encapsulation Mechanism (KEM) introduced in SP 800-227 based on RSASVE from SP 800-56B [29] Note: SP 800-227 as referenced by this document is an Initial Public Draft and is subject to change. Note: TCG_ALG_RSASVE_KEM requires the selection of additional Key Derivation Mechanism (KDM) parameters in order to be used.

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_ECDH_KEM	0x0063	A	NIST SP 800-227 [28]	Key Encapsulation Mechanism (KEM) introduced in SP 800-227 based on C(1e, 1s, ECC CDH) Scheme from SP 800-56A [11] Note: SP 800-227 as referenced by this document is an Initial Public Draft and is subject to change. Note: TCG_ALG_ECDH_KEM requires the selection of additional Key Derivation Mechanism (KDM) parameters in order to be used.
TCG_ALG_LMS	0x0070	A	NIST SP 800-208 [8]	Leighton-Micali Signatures
TCG_ALG_XMSS	0x0071	A	NIST SP 800-208 [8]	eXtended Merkle Signature Scheme (single tree)
TCG_ALG_LMOTS	0x0072	A	NIST SP 800-208 [8]	Leighton-Micali One-Time Signature (used by LMS)
TCG_ALG_WOTSP	0x0073	A	NIST SP 800-208 [8]	Winternitz One-Time Signature Plus (used by XMSS)
TCG_ALG_KEYEDXOF	0x0080	A		any keyed XOF
TCG_ALG_KMACXOF128	0x0081	A	NIST SP 800-185 [30]	
TCG_ALG_KMACXOF256	0x0082	A	NIST SP 800-185 [30]	
TCG_ALG_KMAC128	0x0090	A	NIST SP 800-185 [30]	
TCG_ALG_KMAC256	0x0091	A	NIST SP 800-185 [30]	
TCG_ALG_MLKEM	0x00A0	A	NIST FIPS 203 [31]	ML-KEM
TCG_ALG_MLDSA	0x00A1	A	NIST FIPS 204 [32]	ML-DSA
TCG_ALG_HASH_MLDSA	0x00A2	A	NIST FIPS 204 [32]	HashML-DSA
TCG_ALG_SLHDSA	0x00A3	A	NIST FIPS 205 [33]	SLH-DSA
TCG_ALG_HASH_SLHDSA	0x00A4	A	NIST FIPS 205 [33]	HashSLH-DSA

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
TCG_ALG_ASCON_AEAD	0x00B0	A	NIST SP 800-232 [34]	Authenticated Encryption with Associated Data (AEAD) with 128-bit or 256-bit keys and tag lengths between 64 bits and 128 bits based on Ascon Note: SP 800-232 as referenced by this document is an Initial Public Draft and is subject to change.
TCG_ALG_ASCON_HASH256	0x00B1	A	NIST SP 800-232 [34]	256-bit hash function based on Ascon Note: SP 800-232 as referenced by this document is an Initial Public Draft and is subject to change.
TCG_ALG_ASCON_XOF128	0x00B2	A	NIST SP 800-232 [34]	Extendable-output function (XOF) targeting 128-bit security strength based on Ascon Note: SP 800-232 as referenced by this document is an Initial Public Draft and is subject to change.
TCG_ALG_ASCON_CXOF128	0x00B3	A	NIST SP 800-232 [34]	Customizeable XOF, which incorporates a customization string for domain separation, targeting 128-bit security strength, based on Ascon Note: SP 800-232 as referenced by this document is an Initial Public Draft and is subject to change.
reserved	0x00C1 to 0x00C6			reserved to prevent any overlap with the command structure tags used in TPM 1.2

(continued on next page)

(continued from previous page)

Algorithm Name	Value	C	Reference	Comments
reserved	0x8000 to 0xFFFF			reserved for other structure tags

3 TCG_ECC_CURVE Values

Table 3 is the list of identifiers for TCG-registered curve ID values for elliptic curve cryptography.

Table 3: Definition of (UINT16) TCG_ECC_CURVE Constants

Name	Value	Classification	Comments
TCG_ECC_NONE	0x0000	Assigned	
TCG_ECC_NIST_P192	0x0001	Assigned	
TCG_ECC_NIST_P224	0x0002	Assigned	
TCG_ECC_NIST_P256	0x0003	TCG Standard	
TCG_ECC_NIST_P384	0x0004	TCG Standard	
TCG_ECC_NIST_P521	0x0005	Assigned	
TCG_ECC_BN_P256	0x0010	TCG Standard	curve to support ECDAA
TCG_ECC_BN_P638	0x0011	Assigned	curve to support ECDAA
TCG_ECC_SM2_P256	0x0020	Assigned	
TCG_ECC_BP_P256_R1	0x0030	Assigned	Brainpool
TCG_ECC_BP_P384_R1	0x0031	Assigned	Brainpool
TCG_ECC_BP_P512_R1	0x0032	Assigned	Brainpool
TCG_ECC_CURVE_25519	0x0040	Assigned	curve to support EdDSA
TCG_ECC_CURVE_448	0x0041	Assigned	curve to support EdDSA

4 TCG_MLKEM_PARAMETER_SET Values

Table 4 is the list of parameter sets for use with TCG_ALG_MLKEM.

Table 4: Definition of (UINT16) TCG_MLKEM_PARAMETER_SET Constants

Name	Value	Reference
TCG_MLKEM_NONE	0x0000	n/a
TCG_MLKEM_512	0x0001	NIST FIPS 203
TCG_MLKEM_768	0x0002	NIST FIPS 203
TCG_MLKEM_1024	0x0003	NIST FIPS 203

5 TCG_MLDSA_PARAMETER_SET Values

Table 5 is the list of parameter sets for use with TCG_ALG_MLDSA and TCG_ALG_HASH_MLDSA.

Table 5: Definition of (UINT16) TCG_MLDSA_PARAMETER_SET Constants

Name	Value	Reference
TCG_MLDSA_NONE	0x0000	n/a
TCG_MLDSA_44	0x0001	NIST FIPS 204
TCG_MLDSA_65	0x0002	NIST FIPS 204
TCG_MLDSA_87	0x0003	NIST FIPS 204

6 TCG_SLHDSA_PARAMETER_SET Values

Table 6 is the list of parameter sets for use with TCG_ALG_SLHDSA and TCG_ALG_HASH_SLHDSA.

Table 6: Definition of (UINT16) TCG_SLHDSA_PARAMETER_SET Constants

Name	Value	Reference
TCG_SLHDSA_NONE	0x0000	n/a
TCG_SLHDSA_SHA2_128S	0x0001	NIST FIPS 205
TCG_SLHDSA_SHAKE_128S	0x0002	NIST FIPS 205
TCG_SLHDSA_SHA2_128F	0x0003	NIST FIPS 205
TCG_SLHDSA_SHAKE_128F	0x0004	NIST FIPS 205
TCG_SLHDSA_SHA2_192S	0x0005	NIST FIPS 205
TCG_SLHDSA_SHAKE_192S	0x0006	NIST FIPS 205
TCG_SLHDSA_SHA2_192F	0x0007	NIST FIPS 205
TCG_SLHDSA_SHAKE_192F	0x0008	NIST FIPS 205
TCG_SLHDSA_SHA2_256S	0x0009	NIST FIPS 205
TCG_SLHDSA_SHAKE_256S	0x000A	NIST FIPS 205
TCG_SLHDSA_SHA2_256F	0x000B	NIST FIPS 205
TCG_SLHDSA_SHAKE_256F	0x000C	NIST FIPS 205

7 Hash Algorithms Bit Field

Table 7 defines a bit field to concisely convey a set of hash algorithms. An example of where this could be useful is a parameter returning the set of hash algorithms an interface supports.

Table 7: Definition of (UINT32) TPMA_HASH_ALGS Bits

Bit	Name	Action
0	hashAlgSHA1	SET (1): indicates the SHA1 hash algorithm CLEAR (0): does not indicate SHA1
1	hashAlgSHA256	SET (1): indicates the SHA256 hash algorithm CLEAR (0): does not indicate SHA256
2	hashAlgSHA384	SET (1): indicates the SHA384 hash algorithm CLEAR (0): does not indicate SHA384
3	hashAlgSHA512	SET (1): indicates the SHA512 hash algorithm CLEAR (0): does not indicate SHA512
4	hashAlgSM3_256	SET (1): indicates the SM3_256 hash algorithm CLEAR (0): does not indicate SM3_256
5	hashAlgSHA3_256	SET (1): indicates the SHA3_256 hash algorithm CLEAR (0): does not indicate SHA3_256
6	hashAlgSHA3_384	SET (1): indicates the SHA3_384 hash algorithm CLEAR (0): does not indicate SHA3_384
7	hashAlgSHA3_512	SET (1): indicates the SHA3_512 hash algorithm CLEAR (0): does not indicate SHA3_512
31 to 8	reserved	

Appendices

A Change History

Version	Date	Description
1.27	2017/09/26	Added change history. CMAC algorithm assigned as 0x003F in Table 3. Removed extra whitespace above the title of clause 6.10. Assigned bitfields in Table 26 for SHA3_256, SHA3_384, and SHA3_512. Replaced references of deprecated IETF 3447 with IETF 8017. Removed Annex A (Applicability of this Registry for Other TCG Specifications)
1.28	2020/01/28	Removed Type “H” for TCG_ALG_OAEP in Table 3 Added Types “E” and “M” and comments for TCG_ALG_SM2 in Table 3 Changed references for SM2 to GB/T 32918 Parts 1 through 5 Changed reference for SM3 to ISO/IEC 10118-3:2018 Changed reference for SM4 to GB/T 32907-2016
1.29	2020/02/19	Added algorithms CCM, GCM, KW, KWP, EAX, EdDSA in Table 3 Added Brainpool P256/384/512 R1 curves in Table 4 Added curve parameters for Brainpool P256/384/512 R1 to clause 5.2 Added curve parameters for Curve 25519 to clause 5.2
1.30	2020/02/27	Added 2nd reference to TCG_ALG_ECDH in Table 3 to include X25519 Added note to TCG_ALG_EDDSA in Table 3
1.31	2020/03/09	Updated EDDSA to EdDSA in Table 4 Fixed formatting in Table 5, NIST_P192, parameter value of gY Fixed formatting in Table 10, BN_P256, parameter value of p and n Fixed formatting in Table 18, 19, 20
1.32	2020/03/20	Added new references to bibliography
1.33	2023/03/01	Added LMS, XMSS Added SHAKE128, SHAKE256 and fixed-length variants of SHAKE256 Added SHA256_192 Added EDDSA_PH for HashEdDSA Added CURVE_448 Fixed usage of ‘H’ in some ECC curve parameters (should be ‘h’) Removed mandatory signing scheme from Edwards curve parameter tables Updated references to ISO 10118-3

(continued on next page)

(continued from previous page)

Version	Date	Description
1.34	2023/04/13	Clarified that 'S' applies only to symmetric block ciphers Introduce type 'K' for non-block cipher symmetric functions, adding it to TCG_ALG_HMAC but not the KDFs (to avoid breaking the TPM Library Specification's usage of !ALG.HM) Added KEYEDXOF, KMACXOF128, KMACXOF256, KMAC128, KMAC256 Added type 'H' back to TCG_ALG_OAEP Add note that TCG_ALG_ECDSA is nondeterministic ECDSA
1.35	2023/08/26	Marked 3DES and SHA1 as TCG Legacy
2.0	2025/07/28	Converted document to Markdown. Removed irrelevant material in "Conventions." Removed "Dep" and "Type" columns from ALG_ID table. Removed TPM-specific curve parameter values tables. Removed tables of DER-encoded OID values. Removed TPM-specific symmetric cipher key size tables. Migrated to the TCG_ prefix. Introduced TCG_ALG_MLKEM, TCG_ALG_MLDSA, TCG_ALG_HASH_MLDSA, TCG_ALG_SLHDSA, and TCG_ALG_HASH_SLHDSA Marked ECB as TCG Legacy

B Hash-Based Signature Parameters and Considerations

B.1 Introduction

The hash-based signature schemes listed in Table 2 accept the following parameters:

- H , a hash function.
- h , the height of the Merkle tree. h relates to the trade-off between key generation work and the number of signatures that can be produced by the key.
- w is related to the length of the Winternitz chains that compose the signature. LMS and XMSS define this term differently. In TCG specifications, w refers to the number of bits from the hash or checksum that are used in a single Winternitz chain (that is, LMS's definition of w). w relates to the trade-off between signature size and signature generation/verification work.

Note:

This is in contrast to XMSS, where w refers to the actual length of the Winternitz chain, which uses $\log_2(w)$ bits from the hash or checksum. In the NIST parameter sets for XMSS, $w=4$ (LMS definition) is equivalent to $w=16$ (XMSS definition).

B.2 NIST Parameter Sets

In SP 800-208, FIPS approved and NIST recommended the following parameter sets for SHA256 family usage of LMS and XMSS:

Table 8: Parameters for LMS and XMSS Approved in SP 800-208

Name	H	h	w* (LMS definition)	signature size (bytes)
XMSS-SHA2_10_256	SHA256	10	4	2500
XMSS-SHA2_16_256	SHA256	16	4	2692
XMSS-SHA2_20_256	SHA256	20	4	2820
XMSS-SHA2_10_192	SHA256_192	10	4	1492
XMSS-SHA2_16_192	SHA256_192	16	4	1636
XMSS-SHA2_20_192	SHA256_192	20	4	1732
LMS_SHA256_M32_H5	SHA256	5	{1, 2, 4, 8}	1292 (w=8) to 8684 (w=1)
LMS_SHA256_M32_H10	SHA256	10	{1, 2, 4, 8}	1452 (w=8) to 8844 (w=1)
LMS_SHA256_M32_H15	SHA256	15	{1, 2, 4, 8}	1612 (w=8) to 9004 (w=1)
LMS_SHA256_M32_H20	SHA256	20	{1, 2, 4, 8}	1772 (w=8) to 9164 (w=1)
LMS_SHA256_M32_H25	SHA256	25	{1, 2, 4, 8}	1932 (w=8) to 9324 (w=1)
LMS_SHA256_M24_H5	SHA256_192	5	{1, 2, 4, 8}	780 (w=8) to 4956 (w=1)

(continued on next page)

(continued from previous page)

Name	H	h	w* (LMS definition)	signature size (bytes)
LMS_SHA256_M24_H10	SHA256_192	10	{1, 2, 4, 8}	900 (w=8) to 5076 (w=1)
LMS_SHA256_M24_H15	SHA256_192	15	{1, 2, 4, 8}	1020 (w=8) to 5196 (w=1)
LMS_SHA256_M24_H20	SHA256_192	20	{1, 2, 4, 8}	1140 (w=8) to 5316 (w=1)
LMS_SHA256_M24_H25	SHA256_192	25	{1, 2, 4, 8}	1260 (w=8) to 5436 (w=1)

NIST introduced and recommended SHA256_192 (the 192-bit truncated SHA256 hash) for use with both LMS and XMSS for a trade-off of reduced collision resistance for reduced signature size.

Along with the parameter sets for the SHA256 family algorithms, NIST recommended similar parameter sets that use SHAKE256 and SHAKE256/192 (not listed here).

C ECC Curve Parameters

C.1 Introduction

The tables in this section contain the curve parameter data associated with the curves listed in Table 3.

C.2 NIST_P192

Parameter	Value	Description
curveID	TCG_ECC_NIST_P192	Identifier for the curve
keySize	192	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe ff ff ff ff ff ff ff ff	F_p (the modulus)
a	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe ff ff ff ff ff ff ff fc	Coefficient of the linear term in the curve equation
b	0x64 21 05 19 e5 9c 80 e7 0f a7 e9 ab 72 24 30 49 fe b8 de ec c1 46 b9 b1	Constant term for the curve equation
gX	0x18 8d a8 0e b0 30 90 f6 7c bf 20 eb 43 a1 88 00 f4 ff 0a fd 82 ff 10 12	x coordinate of base point G
gY	0x07 19 2b 95 ff c8 da 78 63 10 11 ed 6b 24 cd d5 73 f9 77 a1 1e 79 48 11	y coordinate of base point G
n	0xff ff ff ff ff ff ff ff ff ff ff ff 99 de f8 36 14 6b c9 b1 b4 d2 28 31	order of G
h	1	cofactor

C.3 NIST_P224

Parameter	Value	Description
curveID	TCG_ECC_NIST_P224	Identifier for the curve
keySize	224	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme

(continued on next page)

(continued from previous page)

Parameter	Value	Description
p	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 01	F_p (the modulus)
a	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe ff ff ff ff ff ff ff ff ff ff ff fe	Coefficient of the linear term in the curve equation
b	0xb4 05 0a 85 0c 04 b3 ab f5 41 32 56 50 44 b0 b7 d7 bf d8 ba 27 0b 39 43 23 55 ff b4	Constant term for the curve equation
gX	0xb7 0e 0c bd 6b b4 bf 7f 32 13 90 b9 4a 03 c1 d3 56 c2 11 22 34 32 80 d6 11 5c 1d 21	x coordinate of base point G
gY	0xbd 37 63 88 b5 f7 23 fb 4c 22 df e6 cd 43 75 a0 5a 07 47 64 44 d5 81 99 85 00 7e 34	y coordinate of base point G
n	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff 16 a2 e0 b8 f0 3e 13 dd 29 45 5c 5c 2a 3d	order of G
h	1	cofactor

C.4 NIST_P256

Parameter	Value	Description
curveID	TCG_ECC_NIST_P256	Identifier for the curve
keySize	256	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xff ff ff ff 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff	F_p (the modulus)
a	0xff ff ff ff 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff fc	Coefficient of the linear term in the curve equation
b	0x5a c6 35 d8 aa 3a 93 e7 b3 eb bd 55 76 98 86 bc 65 1d 06 b0 cc 53 b0 f6 3b ce 3c 3e 27 d2 60 4b	Constant term for the curve equation
gX	0x6b 17 d1 f2 e1 2c 42 47 f8 bc e6 e5 63 a4 40 f2 77 03 7d 81 2d eb 33 a0 f4 a1 39 45 d8 98 c2 96	x coordinate of base point G
gY	0x4f e3 42 e2 fe 1a 7f 9b 8e e7 eb 4a 7c 0f 9e 16 2b ce 33 57 6b 31 5e ce cb b6 40 68 37 bf 51 f5	y coordinate of base point G

(continued on next page)

(continued from previous page)

Parameter	Value	Description
n	0xff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff bc e6 fa ad a7 17 9e 84 f3 b9 ca c2 fc 63 25 51	order of G
h	1	cofactor

C.5 NIST_P384

Parameter	Value	Description
curveID	TCG_ECC_NIST_P384	Identifier for the curve
keySize	384	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA384}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff	F_p (the modulus)
a	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff fc	Coefficient of the linear term in the curve equation
b	0xb3 31 2f a7 e2 3e e7 e4 98 8e 05 6b e3 f8 2d 19 18 1d 9c 6e fe 81 41 12 03 14 08 8f 50 13 87 5a c6 56 39 8d 8a 2e d1 9d 2a 85 c8 ed d3 ec 2a ef	Constant term for the curve equation
gX	0xaa 87 ca 22 be 8b 05 37 8e b1 c7 1e f3 20 ad 74 6e 1d 3b 62 8b a7 9b 98 59 f7 41 e0 82 54 2a 38 55 02 f2 5d bf 55 29 6c 3a 54 5e 38 72 76 0a b7	x coordinate of base point G
gY	0x36 17 de 4a 96 26 2c 6f 5d 9e 98 bf 92 92 dc 29 f8 f4 1d bd 28 9a 14 7c e9 da 31 13 b5 f0 b8 c0 0a 60 b1 ce 1d 7e 81 9d 7a 43 1d 7c 90 ea 0e 5f	y coordinate of base point G
n	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff c7 63 4d 81 f4 37 2d df 58 1a 0d b2 48 b0 a7 7a ec ec 19 6a cc c5 29 73	order of G
h	1	cofactor

C.6 NIST_P521

Parameter	Value	Description
curveID	TCG_ECC_NIST_P521	Identifier for the curve

(continued on next page)

(continued from previous page)

Parameter	Value	Description
keySize	521	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA512}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0x01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	F_p (the modulus)
a	0x01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fc	Coefficient of the linear term in the curve equation
b	0x00 51 95 3e b9 61 8e 1c 9a 1f 92 9a 21 a0 b6 85 40 ee a2 da 72 5b 99 b3 15 f3 b8 b4 89 91 8e f1 09 e1 56 19 39 51 ec 7e 93 7b 16 52 c0 bd 3b b1 bf 07 35 73 df 88 3d 2c 34 f1 ef 45 1f d4 6b 50 3f 00	Constant term for the curve equation
gX	0x00 c6 85 8e 06 b7 04 04 e9 cd 9e 3e cb 66 23 95 b4 42 9c 64 81 39 05 3f b5 21 f8 28 af 60 6b 4d 3d ba a1 4b 5e 77 ef e7 59 28 fe 1d c1 27 a2 ff a8 de 33 48 b3 c1 85 6a 42 9b f9 7e 7e 31 c2 e5 bd 66	x coordinate of base point G
gY	0x01 18 39 29 6a 78 9a 3b c0 04 5c 8a 5f b4 2c 7d 1b d9 98 f5 44 49 57 9b 44 68 17 af bd 17 27 3e 66 2c 97 ee 72 99 5e f4 26 40 c5 50 b9 01 3f ad 07 61 35 3c 70 86 a2 72 c2 40 88 be 94 76 9f d1 66 50	y coordinate of base point G
n	0x01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fa 51 86 87 83 bf 2f 96 6b 7f cc 01 48 f7 09 a5 d0 3b b5 c9 b8 89 9c 47 ae bb 6f b7 1e 91 38 64 09	order of G
h	1	cofactor

C.7 BN_P256

Parameter	Value	Description
curveID	TCG_ECC_BN_P256	Identifier for the curve
keySize	256	Size in bits of the key
kdf	{TCG_ALG_NULL, TCG_ALG_NULL}	The default KDF and hash

(continued on next page)

(continued from previous page)

Parameter	Value	Description
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xff ff ff ff ff fc f0 cd 46 e5 f2 5e ee 71 a4 9f 0c dc 65 fb 12 98 0a 82 d3 29 2d db ae d3 30 13	F_p (the modulus)
a	0	Coefficient of the linear term in the curve equation
b	3	Constant term for the curve equation
gX	1	x coordinate of base point G
gY	2	y coordinate of base point G
n	0xff ff ff ff ff fc f0 cd 46 e5 f2 5e ee 71 a4 9e 0c dc 65 fb 12 99 92 1a f6 2d 53 6c d1 0b 50 0d	order of G
h	1	cofactor

C.8 BN_P638

Parameter	Value	Description
curveID	TCG_ECC_BN_P638	Identifier for the curve
keySize	638	Size in bits of the key
kdf	{TCG_ALG_NULL, TCG_ALG_NULL}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0x23 ff ff fd c0 00 00 0d 7f ff ff b8 00 00 01 d3 ff ff f9 42 d0 00 16 5e 3f ff 94 87 00 00 d5 2f ff fd d0 e0 00 08 de 55 c0 00 86 52 00 21 e5 5b ff ff f5 1f ff f4 eb 80 00 00 00 4c 80 01 5a cd ff ff ff ff ff ff ff ec e0 00 00 00 00 00 00 00 67	F_p (the modulus)
a	0	Coefficient of the linear term in the curve equation

(continued on next page)

(continued from previous page)

Parameter	Value	Description
b	0x01 01	Constant term for the curve equation
gX	0x23 ff ff fd c0 00 00 0d 7f ff ff b8 00 00 01 d3 ff ff f9 42 d0 00 16 5e 3f ff 94 87 00 00 d5 2f ff fd d0 e0 00 08 de 55 c0 00 86 52 00 21 e5 5b ff ff f5 1f ff f4 eb 80 00 00 00 4c 80 01 5a cd ff ff ff ff ff ff ff ec e0 00 00 00 00 00 00 66	x coordinate of base point G
gY	0x10	y coordinate of base point G
n	0x23 ff ff fd c0 00 00 0d 7f ff ff b8 00 00 01 d3 ff ff f9 42 d0 00 16 5e 3f ff 94 87 00 00 d5 2f ff fd d0 e0 00 08 de 55 60 00 86 55 00 21 e5 55 ff ff f5 4f ff f4 ea c0 00 00 00 49 80 01 54 d9 ff ff ff ff ff ff ff ed a0 00 00 00 00 00 00 61	order of G
h	1	cofactor

C.9 SM2_P256

Parameter	Value	Description
curveID	TCG_ECC_SM2_P256	Identifier for the curve
keySize	256	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SM3_256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xff ff ff fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff	F_p (the modulus)
a	0xff ff ff fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff fc	Coefficient of the linear term in the curve equation
b	0x28 e9 fa 9e 9d 9f 5e 34 4d 5a 9e 4b cf 65 09 a7 f3 97 89 f5 15 ab 8f 92 dd bc bd 41 4d 94 0e 93	Constant term for the curve equation
gX	0x32 c4 ae 2c 1f 19 81 19 5f 99 04 46 6a 39 c9 94 8f e3 0b bf f2 66 0b e1 71 5a 45 89 33 4c 74 c7	x coordinate of base point G
gY	0xbc 37 36 a2 f4 f6 77 9c 59 bd ce e3 6b 69 21 53 d0 a9 87 7c c6 2a 47 40 02 df 32 e5 21 39 f0 a0	y coordinate of base point G

(continued on next page)

(continued from previous page)

Parameter	Value	Description
n	0xff ff ff fe ff ff ff ff ff ff ff ff ff ff 72 03 df 6b 21 c6 05 2b 53 bb f4 09 39 d5 41 23	order of G
h	1	cofactor

C.10 BP_P256_R1

Parameter	Value	Description
curveID	TCG_ECC_BP_P256_R1	Identifier for the curve
keySize	256	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xa9 fb 57 db a1 ee a9 bc 3e 66 0a 90 9d 83 8d 72 6e 3b f6 23 d5 26 20 28 20 13 48 1d 1f 6e 53 77	F_p (the modulus)
a	0x7d 5a 09 75 fc 2c 30 57 ee f6 75 30 41 7a ff e7 fb 80 55 c1 26 dc 5c 6c e9 4a 4b 44 f3 30 b5 d9	Coefficient of the linear term in the curve equation
b	0x26 dc 5c 6c e9 4a 4b 44 f3 30 b5 d9 bb d7 7c bf 95 84 16 29 5c f7 e1 ce 6b cc dc 18 ff 8c 07 b6	Constant term for the curve equation
gX	0x8b d2 ae b9 cb 7e 57 cb 2c 4b 48 2f fc 81 b7 af b9 de 27 e1 e3 bd 23 c2 3a 44 53 bd 9a ce 32 62	x coordinate of base point G
gY	0x54 7e f8 35 c3 da c4 fd 97 f8 46 1a 14 61 1d c9 c2 77 45 13 2d ed 8e 54 5c 1d 54 c7 2f 04 69 97	y coordinate of base point G
n	0xa9 fb 57 db a1 ee a9 bc 3e 66 0a 90 9d 83 8d 71 8c 39 7a a3 b5 61 a6 f7 90 1e 0e 82 97 48 56 a7	order of G
h	1	cofactor

C.11 BP_P384_R1

Parameter	Value	Description
curveID	TCG_ECC_BP_P384_R1	Identifier for the curve
keySize	384	Size in bits of the key

(continued on next page)

(continued from previous page)

Parameter	Value	Description
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA384}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0x8c b9 1e 82 a3 38 6d 28 0f 5d 6f 7e 50 e6 41 df 15 2f 71 09 ed 54 56 b4 12 b1 da 19 7f b7 11 23 ac d3 a7 29 90 1d 1a 71 87 47 00 13 31 07 ec 53	F_p (the modulus)
a	0x7b c3 82 c6 3d 8c 15 0c 3c 72 08 0a ce 05 af a0 c2 be a2 8e 4f b2 27 87 13 91 65 ef ba 91 f9 0f 8a a5 81 4a 50 3a d4 eb 04 a8 c7 dd 22 ce 28 26	Coefficient of the linear term in the curve equation
b	0x04 a8 c7 dd 22 ce 28 26 8b 39 b5 54 16 f0 44 7c 2f b7 7d e1 07 dc d2 a6 2e 88 0e a5 3e eb 62 d5 7c b4 39 02 95 db c9 94 3a b7 86 96 fa 50 4c 11	Constant term for the curve equation
gX	0x1d 1c 64 f0 68 cf 45 ff a2 a6 3a 81 b7 c1 3f 6b 88 47 a3 e7 7e f1 4f e3 db 7f ca fe 0c bd 10 e8 e8 26 e0 34 36 d6 46 aa ef 87 b2 e2 47 d4 af 1e	x coordinate of base point G
gY	0x8a be 1d 75 20 f9 c2 a4 5c b1 eb 8e 95 cf d5 52 62 b7 0b 29 fe ec 58 64 e1 9c 05 4f f9 91 29 28 0e 46 46 21 77 91 81 11 42 82 03 41 26 3c 53 15	y coordinate of base point G
n	0x8c b9 1e 82 a3 38 6d 28 0f 5d 6f 7e 50 e6 41 df 15 2f 71 09 ed 54 56 b3 1f 16 6e 6c ac 04 25 a7 cf 3a b6 af 6b 7f c3 10 3b 88 32 02 e9 04 65 65	order of G
h	1	cofactor

C.12 BP_P512_R1

Parameter	Value	Description
curveID	TCG_ECC_BP_P512_R1	Identifier for the curve
keySize	512	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA512}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xaa dd 9d b8 db e9 c4 8b 3f d4 e6 ae 33 c9 fc 07 cb 30 8d b3 b3 c9 d2 0e d6 63 9c ca 70 33 08 71 7d 4d 9b 00 9b c6 68 42 ae cd a1 2a e6 a3 80 e6 28 81 ff 2f 2d 82 c6 85 28 aa 60 56 58 3a 48 f3	F_p (the modulus)

(continued on next page)

(continued from previous page)

Parameter	Value	Description
a	0x78 30 a3 31 8b 60 3b 89 e2 32 71 45 ac 23 4c c5 94 cb dd 8d 3d f9 16 10 a8 34 41 ca ea 98 63 bc 2d ed 5d 5a a8 25 3a a1 0a 2e f1 c9 8b 9a c8 b5 7f 11 17 a7 2b f2 c7 b9 e7 c1 ac 4d 77 fc 94 ca	Coefficient of the linear term in the curve equation
b	0x3d f9 16 10 a8 34 41 ca ea 98 63 bc 2d ed 5d 5a a8 25 3a a1 0a 2e f1 c9 8b 9a c8 b5 7f 11 17 a7 2b f2 c7 b9 e7 c1 ac 4d 77 fc 94 ca dc 08 3e 67 98 40 50 b7 5e ba e5 dd 28 09 bd 63 80 16 f7 23	Constant term for the curve equation
gX	0x81 ae e4 bd d8 2e d9 64 5a 21 32 2e 9c 4c 6a 93 85 ed 9f 70 b5 d9 16 c1 b4 3b 62 ee f4 d0 09 8e ff 3b 1f 78 e2 d0 d4 8d 50 d1 68 7b 93 b9 7d 5f 7c 6d 50 47 40 6a 5e 68 8b 35 22 09 bc b9 f8 22	x coordinate of base point G
gY	0x7d de 38 5d 56 63 32 ec c0 ea bf a9 cf 78 22 fd f2 09 f7 00 24 a5 7b 1a a0 00 c5 5b 88 1f 81 11 b2 dc de 49 4a 5f 48 5e 5b ca 4b d8 8a 27 63 ae d1 ca 2b 2f a8 f0 54 06 78 cd 1e 0f 3a d8 08 92	y coordinate of base point G
n	0xaa dd 9d b8 db e9 c4 8b 3f d4 e6 ae 33 c9 fc 07 cb 30 8d b3 b3 c9 d2 0e d6 63 9c ca 70 33 08 70 55 3e 5c 41 4c a9 26 19 41 86 61 19 7f ac 10 47 1d b1 d3 81 08 5d da dd b5 87 96 82 9c a9 00 69	order of G
h	1	cofactor

C.13 CURVE 25519

Note:

The gY value for Curve25519 is one of two distinct yet compatible possible values. The other value for gY begins with 0x20 ae 19 a1.

Parameter	Value	Description
curveID	TCG_ECC_CURVE_25519	Identifier for the curve
keySize	256	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0x7f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ed	F_p (the modulus)

(continued on next page)

(continued from previous page)

Parameter	Value	Description
a	0x07 6d 06	Coefficient of the linear term in the curve equation
b	1	Constant term for the curve equation
gX	9	x coordinate of base point G
gY	0x5f 51 e6 5e 47 5f 79 4b 1f e1 22 d3 88 b7 2e b3 6d c2 b2 81 92 83 9e 4d d6 16 3a 5d 81 31 2c 14	y coordinate of base point G
n	0x10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 de f9 de a2 f7 9c d6 58 12 63 1a 5c f5 d3 ed	order of G
h	8	cofactor

C.14 CURVE 448

Parameter	Value	Description
curveID	TCG_ECC_CURVE_448	Identifier for the curve
keySize	448	Size in bits of the key
kdf	{TCG_ALG_KDF1_SP800_56A, TCG_ALG_SHA256}	The default KDF and hash
sign	{TCG_ALG_NULL, TCG_ALG_NULL}	No mandatory signing scheme
p	0xff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	F_p (the modulus)
a	0x02 62 a6	Coefficient of the linear term in the curve equation
b	1	Constant term for the curve equation
gX	5	x coordinate of base point G
gY	0x7d 23 5d 12 95 f5 b1 f6 6c 98 ab 6e 58 32 6f ce cb ae 5d 34 f5 55 45 d0 60 f7 5d c2 8d f3 f6 ed b8 02 7e 23 46 43 0d 21 13 12 c4 b1 50 67 7a f7 6f d7 22 3d 45 7b 5b 1a	y coordinate of base point G

(continued on next page)

(continued from previous page)

Parameter	Value	Description
n	0x3f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 7c ca 23 e9 c4 4e db 49 ae d6 36 90 21 6c c2 72 8d c5 8f 55 23 78 c2 92 ab 58 44 f3	order of G
h	1	cofactor

D Hash Parameters

D.1 Introduction

The tables in this clause define the basic parameters associated with the TCG-registered hash algorithms listed in Table 2.

D.2 SHA1

Parameter	Value	Description
Digest Size	20	Size of digest in octets
Block Size	64	Size of hash block in octets
OID (DER)	0x30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14	

D.3 SHA256

Parameter	Value	Description
Digest Size	32	Size of digest in octets
Block Size	64	Size of hash block in octets
OID (DER)	0x30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20	

D.4 SHA384

Parameter	Value	Description
Digest Size	48	Size of digest in octets
Block Size	128	Size of hash block in octets
OID (DER)	0x30 41 30 0d 06 09 60 86 48 01 65 03 04 02 02 05 00 04 30	

D.5 SHA512

Parameter	Value	Description
Digest Size	64	Size of digest in octets
Block Size	128	Size of hash block in octets
OID (DER)	0x30 51 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 04 40	

D.6 SM3_256

Parameter	Value	Description
Digest Size	32	Size of digest in octets
Block Size	64	Size of hash block in octets
OID (DER)	0x30 30 30 0c 06 08 2a 81 1c 81 45 01 83 11 05 00 04 20	

D.7 SHA3_256

Parameter	Value	Description
Digest Size	32	Size of digest in octets
Block Size	136	Size of hash block in octets
OID (DER)	0x30 31 30 0d 06 09 60 86 48 01 65 03 04 02 08 05 00 04 20	

D.8 SHA3_384

Parameter	Value	Description
Digest Size	48	Size of digest in octets
Block Size	104	Size of hash block in octets
OID (DER)	0x30 41 30 0d 06 09 60 86 48 01 65 03 04 02 09 05 00 04 30	

D.9 SHA3_512

Parameter	Value	Description
Digest Size	64	Size of digest in octets
Block Size	72	Size of hash block in octets
OID (DER)	0x30 51 30 0d 06 09 60 86 48 01 65 03 04 02 0a 05 00 04 40	

References

- [1] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, "RFC 8017 - PKCS #1: RSA Cryptography Specifications Version 2.2." RFC Editor, Nov. 2016. Available: <https://www.rfc-editor.org/info/rfc8017>
- [2] "Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers." ISO/IEC, Dec. 2010. Available: <https://www.iso.org/standard/54531.html>
- [3] "IT Security techniques - Hash-functions - Part 3: Dedicated hash-functions." ISO/IEC, Oct. 2018. Available: <https://www.iso.org/standard/67116.html>
- [4] "Information security - Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function." ISO/IEC, Jun. 2021. Available: <https://www.iso.org/standard/75296.html>
- [5] "IEEE Standard Specifications for Public-Key Cryptography." IEEE, Aug. 2000. Available: <https://standards.ieee.org/ieee/1363/2049/>
- [6] "IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques." IEEE, Sep. 2004. Available: <https://standards.ieee.org/ieee/1363a/2050/>
- [7] "Trusted Platform Module 2.0 Library." Trusted Computing Group, Mar. 2024. Available: <https://trustedcomputinggroup.org/resource/tpm-library-specification/>
- [8] C. Miller, "SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes." National Institute of Standards and Technology, Oct. 2020. Available: <https://csrc.nist.gov/pubs/sp/800/208/final>
- [9] "SM4 Block Cipher Algorithm." Standardization Administration of the PRC, 2016.
- [10] "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms." ISO/IEC, Nov. 2018. Available: <https://www.iso.org/standard/76382.html>
- [11] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, "SP 800-56A: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography." National Institute of Standards and Technology, Apr. 2018. Available: http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf
- [12] A. Langley, M. Hamburg, and S. Turner, "RFC 7748: Elliptic Curves for Security." RFC Editor, Jan. 2016. Available: <https://www.rfc-editor.org/info/rfc7748>
- [13] "Information Security Technology - Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves - Part 1: General." Standardization Administration of the PRC, 2016. Available: <https://webstore.ansi.org/standards/spc/gb329182016>
- [14] "Information Security Technology - Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves - Part 2: Digital Signature Algorithm." Standardization Administration of the PRC, 2016.
- [15] "Information Security Technology - Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves - Part 3: Key exchange protocol." Standardization Administration of the PRC, 2016.
- [16] "Information Security Technology - Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves - Part 4: Public key encryption algorithm." Standardization Administration of the PRC, 2016.
- [17] "Information Security Technology - Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves - Part 5: Parameter definition." Standardization Administration of the PRC, 2016.
- [18] H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)." RFC Editor, May 2010. Available: <https://www.rfc-editor.org/info/rfc5869>
- [19] L. Chen, "SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions." National Institute of Standards and Technology, Aug. 2022. Available: <http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf>
- [20] "Information technology - Security techniques - Cryptographic techniques based on elliptic curves." ISO/IEC, Jul. 2016. Available: <https://www.iso.org/standard/65480.html>
- [21] S. Josefsson and I. Liusvaara, "RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)." RFC Editor, Jan. 2017. Available: <https://www.rfc-editor.org/info/rfc8032>
- [22] "Information security - Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher." ISO/IEC, Mar. 2011. Available: <https://www.iso.org/standard/50375.html>

- [23] “Information technology - Security techniques - Modes of operation for an n-bit block cipher.” ISO/IEC, Jul. 2017. Available: <https://www.iso.org/standard/64575.html>
- [24] M. Dworkin, “SP 800-38C: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality.” National Institute of Standards and Technology, May 2004. Available: <https://csrc.nist.gov/pubs/sp/800/38/c/upd1/final>
- [25] M. Dworkin, “SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.” National Institute of Standards and Technology, Nov. 2007. Available: <https://csrc.nist.gov/pubs/sp/800/38/d/final>
- [26] M. Dworkin, “SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.” National Institute of Standards and Technology, Dec. 2012. Available: <https://csrc.nist.gov/pubs/sp/800/38/f/final>
- [27] “Information security - Authenticated encryption.” ISO/IEC, Nov. 2020. Available: <https://www.iso.org/standard/81550.html>
- [28] G. Alagic *et al.*, “SP 800-227: Recommendations for Key-Encapsulation Mechanisms.” Jan. 2025. Available: <https://csrc.nist.gov/pubs/sp/800/227/ipd>
- [29] E. Barker, L. Chen, A. Roginsky, A. Vassilev, R. Davis, and S. Simon, “SP 800-56B: Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography.” National Institute of Standards and Technology, Mar. 2019. Available: <https://csrc.nist.gov/pubs/sp/800/56/b/r2/final>
- [30] J. Kelsey, S. Chang, and R. Perlner, “SP 800-185: SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash.” National Institute of Standards and Technology, Dec. 2016. Available: <https://csrc.nist.gov/pubs/sp/800/185/final>
- [31] “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.” National Institute of Standards and Technology, Aug. 2024. Available: <https://csrc.nist.gov/pubs/fips/203/final>
- [32] “FIPS 204: Module-Lattice-Based Digital Signature Standard.” National Institute of Standards and Technology, Aug. 2024. Available: <https://csrc.nist.gov/pubs/fips/204/final>
- [33] “FIPS 205: Stateless Hash-Based Digital Signature Standard.” National Institute of Standards and Technology, Aug. 2024. Available: <https://csrc.nist.gov/pubs/fips/205/final>
- [34] M. S. Turan, K. A. McKay, D. Chang, J. Kang, and J. Kelsey, “SP 800-232: Ascon-Based Lightweight Cryptography Standards for Constrained Devices.” Nov. 2024. Available: <https://csrc.nist.gov/pubs/sp/800/232/ipd>