TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.xxxx-Part2 제정일: 2018년 12월 xx일

패스워드 기반 키 유도 함수 - 제2부: 해시 함수 SHA-2

Password-based Key Derivation Function - Part2: Hash Function SHA-2

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 정보보호기반 프로젝트그룹(PG501)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part2
표준 초안 작성자	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part2
	주왕호	NSR	연구원	-	TTAK.KO-12.xxxx-Part2
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

서 문

1 표준의 목적

이 표준은 패스워드(또는 패스프레이즈)를 입력으로 하여 암호 키를 생성하는 키 유도 함수에 해시 함수 SHA-2를 적용할 경우의 참조 구현값을 제시하여, 패스워드 기반 키 유도 함수의 구현 정확성을 확인할 수 있도록 한다.

2 주요 내용 요약

이 표준은 패스워드 기반 키 유도 함수의 기반 해시 함수로 SHA-2를 적용할 경우의 참조 구현값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 제1부 일반에 규정된 패스워드 기반 키 유도 함수의 기반 해시 함수로 ISO/IEC 10118-3에 규정된 해시 함수 SHA-2를 적용한 결과로, 패스워드 기반 키 유도 함수와 SHA-2는 각 표준의 상세 규격을 준용한다.

3.2 인용 표준과 본 표준의 비교표

- 해당없음

Preface

1 Purpose

The standard provides test vectors of KDF, used as a password(or passphase) based on SHA-2 about implementation conformance.

2 Summary

The standard specifies the test vectors of PBKDF based on SHA-2 about implementation conformance

3 Comparison to Reference Standards

3.1 Relationship to Reference Standards

The test vectors in this standard are result of applying the hash function SHA-2 specified in ISO/IEC 10118-3, the PBKDF mechanism specified in Part 1: General. And, PBKDF and SHA-2 conform to the specifications of each standard.

목 차

패스워드 기반 키 유도 함수
- 제2부: 해시 함수 SHA-2
(Password-based Key Derivation Function)
- Part2: Hash Function SHA-2)

1 적용 범위

제1부에서 정의한 패스워드 기반 키 유도 함수는 HMAC을 기반 함수로 사용한다. 이 표준은 HMAC의 기반 해시 함수로 SHA-2를 적용하는 패스워드 기반 키 유도 함수의 참조 구현값을 제시한다. 참조 구현값 생성에 사용된 해시 함수는 <표 1-1>과 같다.

<표 1-1> 패스워드 기반 키 유도 함수의 참조 구현값 생성에 사용되는 해시 함수

해시 함수	SHA-224	SHA-256	SHA-384	SHA-512
출력 블록 크기 hLen (비트)	224	256	384	512

HMAC 기반 키 유도 함수는 HMAC을 의사 난수 함수(PRF)로 사용한다. HMAC에 적용하는 해시 함수에 따라 의사 난수 함수를 구분하면 <표 1-2>와 같다.

<표 1-2> PRF 알고리즘

구분	알고리즘	
의사 난수 함수 (PRF)	HMAC-SHA2	HMAC-SHA-224
		HMAC-SHA-256
		HMAC-SHA-384
		HMAC-SHA-512

2 인용 표준

- TTAK.KO-12.0xxx-Part1, “패스워드 기반 키 유도 함수 - 제1부 일반”, 2018. 12.
  (※ 이 표준의 용어 정의, 약어 및 기호는 해당 표준을 따름)

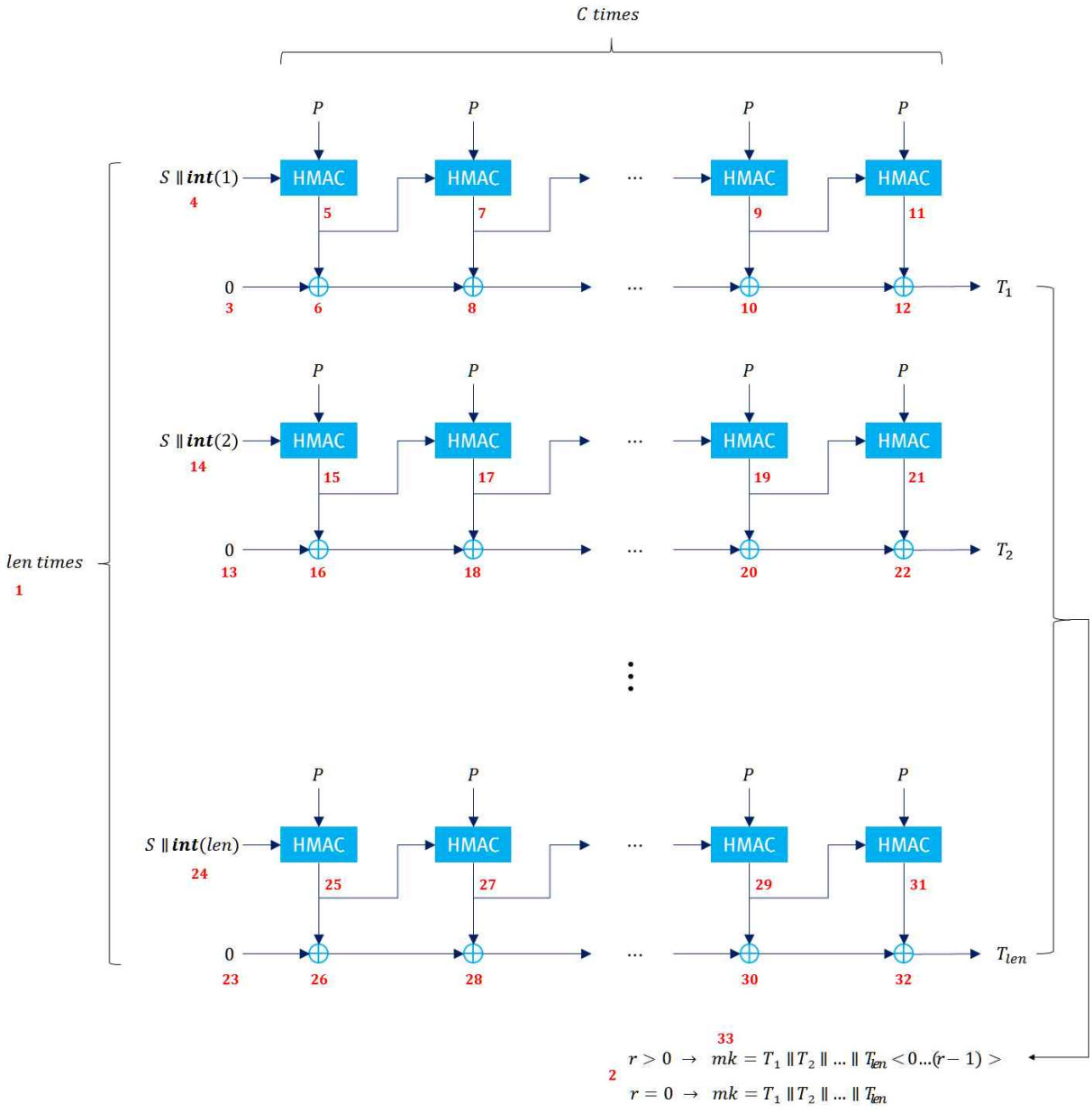
3 용어 정의

- 해당없음

4 약어

- 해당없음

5 참조 구현값



5.1 HMAC-SHA-224의 단계별 참조 구현값

입력	P (문자열)	TTAK0!HellowWorld!SHA2224
	S (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	C (10진수)	2048
	kLen (10진수)	672

위치	변수	중간값(16진수)
1	len	3
2	r	0
3	T_1	0
4	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000001
5	U_1	b926d238e95cd85f882f65a7de58021fbae70108a81ee340215d9d0d
6	T_1	b926d238e95cd85f882f65a7de58021fbae70108a81ee340215d9d0d
7	U_2	e139707d990dc68ddab4079a90dc9a5f754cd971a21b72230ffa0a82
8	T_1	581fa24570511ed2529b623d4e849840cfabd8790a0591632ea7978f
9	U_{c-1}	26f57a4c6edf6f3ac78c529a7be7403fc53089c7a1574412338710a2
10	T_1	ae882c359adc1fe8b850f7e6f88cb2669ae40e78220e3fea7ac4a1a2
11	U_c	731922e44fe01c8cfc6f6dfe3841eb41fa3c30e41542e06928622ddf
12	T_1	dd910ed1d53c0364443f9a18c0cd592760d83e9c374cdf8352a68c7d
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000002
15	U_1	40de509c93532151a66684fb65cedf7c440d0774640bf8cc4a36a25f
16	T_2	40de509c93532151a66684fb65cedf7c440d0774640bf8cc4a36a25f
17	U_2	264c8a7e693a1c000d4d6e4a0ccaf3d5132d3a42c1c0249561528d18
18	T_2	6692dae2fa693d51ab2beab169042ca957203d36a5cbdc592b642f47
19	U_{c-1}	8a8d545a71c7b11df61cd21cba0bbd4b8333054b4e22102c08dca571
20	T_2	0d463123b57a2d78f9974643f48ebffca99ec7f4bd305df57be12535
21	U_c	74b989d17658fc2a76db273bf8d8151e8c099b826820d3b51f98846c
22	T_2	79ffb8f2c322d1528f4c61780c56aae225975c76d5108e406479a159
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000003
25	U_1	7a26a90e71ecbc53e95599897785e2819fe8e883d957408436ee47db
26	T_{len}	7a26a90e71ecbc53e95599897785e2819fe8e883d957408436ee47db
27	U_2	ff89b9a3de59a5e7e20ea8e2e0742d350f545b461e154e9b348e421f
28	T_{len}	85af10adafb519b40b5b316b97f1cfb490bcb3c5c7420e1f026005c4
29	U_{c-1}	28c4240a4fe2fcf40bbdb2706f5f65d095c37c234dfeb22b2fe3bbe2
30	T_{len}	916f4da90acb227fd7314480f940521715988b3ac14e421d9f506332
31	U_c	cabdb01088e31fb5fdfb028152b00e3bd9f57c6445afbd561efb97f8
32	T_{len}	5bd2fdb982283dca2aca4601abf05c2ccc6df75e84e1ff4b81abf4ca
33	mk	dd910ed1d53c0364443f9a18c0cd592760d83e9c374cdf8352a68c7d79ffb8f2c322d1528f4c61780c56aae225975c76d5108e406479a1595bd2fdb982283dca2aca4601abf05c2ccc6df75e84e1ff4b81abf4ca

5.2 HMAC-SHA-256의 단계별 참조 구현값

입력	P (문자열)	TTAK0!HellowWorld!SHA2256
	S (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	C (10진수)	2048
	kLen (10진수)	768

위치	변수	중간값(16진수)
1	len	3
2	r	0
3	T_1	0
4	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000001
5	U_1	89c6d5d632be9e20a243c91d8aad9c7097dbbba7762c61fd97cc51c8efa3c9cc
6	T_1	89c6d5d632be9e20a243c91d8aad9c7097dbbba7762c61fd97cc51c8efa3c9cc
7	U_2	5e887b8612ffc29a16e2a3a115baed001617f41aca3aa3e1a9608fbbde793530
8	T_1	d74eae5020415cbab4a16abc9f17717081cc4fbdbc16c21c3eacde7331dafcfc
9	U_{c-1}	89301430f6bcbbec6f6f24a56720af168851469e33af2fc074c048b6340728d2
10	T_1	7f949848cac85f36c3b68624deec3a62c6689bcf3f39d0dbd98cd93fcce555d8
11	U_c	ecd86afb5ab0867c7a717dd3676e7b8f5c752cd575b99685a0a96b478a03cc7e
12	T_1	934cf2b39078d94ab9c7fbf7b98241ed9a1db71a4a80465e7925b27846e699a6
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000002
15	U_1	5a796b1a92d4d9176bae5fe2a33cfb3cb6fc13b4e2bf535d2d91418348e66989
16	T_2	5a796b1a92d4d9176bae5fe2a33cfb3cb6fc13b4e2bf535d2d91418348e66989
17	U_2	24a134008b44c2fad0de35f8022f40965007582d86fd6a1774ba52a420aa64b0
18	T_2	7ed85f1a19901bedbb706a1aa113bbaae6fb4b996442394a592b1327684c0d39
19	U_{c-1}	8f007c8bcde0310d1667bba4123f9f217dd6b3dd57ee92453f3851185950d61c
20	T_2	5273ee759fe2a865dbf90fdcf6af7ae46b0c1cb132bbff9e54781b604915b5a8
21	U_c	9a0b38e1ec5c041f6d4beb840482b2b4394a2bb552be6831a45839a384206287
22	T_2	c878d69473beac7ab6b2e458f22dc85052463704600597aff02022c3cd35d72f
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	15c54f280c7e4184598cc94b92fbe5a67d62cf871810e00de6eeca1ac3f7e8a3
26	T_{len}	15c54f280c7e4184598cc94b92fbe5a67d62cf871810e00de6eeca1ac3f7e8a3
27	U_2	9ab1823fb2d8f2cc0ba316f47e3241e4ff2c8add41cd6b21fe3a58b6f61aef40
28	T_{len}	8f74cd17bea6b348522fdfbfecc9a442824e455a59dd8b2c18d492ac35ed07e3
29	U_{c-1}	a2d1c72ec8d546c98d2b0b748ad3a57a44753fa85e86591c9f2d77b7247fa3d6
30	T_{len}	99e693b24cf2de411399537f3732b85e7b1e80475609009ac1d67801ea091822
31	U_c	71d577d981891182d09279c3bd26a30b645a080e2b366b8d7507344e26325cac
32	T_{len}	e833e46bcd7bcfc3c30b2abc8a141b551f4488497d3f6b17b4d14c4fcc3b448e
33	mk	934cf2b39078d94ab9c7fbf7b98241ed9a1db71a4a80465e7925b27846e699a6c878d69473beac7ab6b2e458f22dc85052463704600597aff02022c3cd35d72fe833e46bcd7bcfc3c30b2abc8a141b551f4488497d3f6b17b4d14c4fcc3b448e

5.3 HMAC-SHA-384의 단계별 참조 구현값

입력	P (문자열)	TTAK0!HellowWorld!SHA2384
	S (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	C (10진수)	2048
	kLen (10진수)	1152

위치	변수	중간값(16진수)
1	len	3
2	r	0
3	T_1	0
4	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00000001
5	U_1	fd37c4732bef495aa18b9ebe4a92fba69c8819e721c036a23734e3acb8fde044 8768ac54ce0460b74514f3af34ea78f3
6	T_1	fd37c4732bef495aa18b9ebe4a92fba69c8819e721c036a23734e3acb8fde044 8768ac54ce0460b74514f3af34ea78f3
7	U_2	c8f220440336e538baa5d14387d11c75dab279cd540246be40f3edcea381d357 d2dfc0160f401047f382b50e4bdfdcde
8	T_1	35c5e43728d9ac621b2e4ffdcd43e7d3463a602a75c2701c77c70e621b7c3313 55b76c42c14470f0b69646a17f35a42d
9	U_{c-1}	ea670fd3ca986d72e2d955ab3df1753355c8f3a600489909c08d91c2c1d0f6f9 bdf2a6294eec16ded84e3b84c24cf438
10	T_1	438f9884b8630a419465a2f74af5a2ce645c598ee3d5cd9c2eda9d78d923a59d d82e647bce764f01888a6809d4938aa5
11	U_c	4618c4e76b4e26727adcfc7680a01a1a83bc4f425daafae0dd92e33b21b10bca 20b3ba3c4383b6bb52b05bbbf497046a
12	T_1	05975c63d32d2c33eeb95e81ca55b8d4e7e016ccbe7f377cf3487e43f892ae57 f89dde478df5f9bada3a33b220048ecf
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00000002
15	U_1	e3abf746e9d42d96f9b29be978d591e5d65849d9ac8079a89158506a493d639b 1428fa8246dac908dc1aa6061195f74b
16	T_2	e3abf746e9d42d96f9b29be978d591e5d65849d9ac8079a89158506a493d639b 1428fa8246dac908dc1aa6061195f74b
17	U_2	98e48cf27ba8d49bec8068632b4f8f81d444ab1ea10a46ead09652e296d17210 b00211ac27c2ea0968ea0185cb303bd2
18	T_2	7b4f7bb4927cf90d1532f38a539a1e64021ce2c70d8a3f4241ce0288dfec118b a42aeb2e61182301b4f0a783daa5cc99
19	U_{c-1}	9c5c22130ef32fa02accf6886fe361883eb8e4222496ae9e35308a5cc14bf3de f247182d84327f63d5a325a4343d16c7
20	T_2	365d10196c73b350d21e843bce8f9af20b1b1e5b2a49d6c4ca2895cb222f524d c789254c63a1d7570a3c1d1b854f04b2
21	U_c	2a20aa45be61236215b0bceff1413747acadbd4db0815a79e4a7b85017fc84e4 06ea201120791159a982ac4953cb3925
22	T_2	1c7dba5cd2129032c7ae38d43fceadb5a7b6a3169ac88cbd2e8f2d9b35d3d6a9 c163055d43d8c60ea3beb152d6843d97

23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	7ac8ec8c60cd8c0b8f9df0a76ed3016f3bf21e6f5e0483d29f34b4ab4d01921b8ad97e1ab9634f9875c584d9da124345
26	T_{len}	7ac8ec8c60cd8c0b8f9df0a76ed3016f3bf21e6f5e0483d29f34b4ab4d01921b8ad97e1ab9634f9875c584d9da124345
27	U_2	409dd2838f2e650f57a51850962 1a41797ade0796b6eaaf5d89acb5349fbbc532ed2eaa32a9c4f426d248f5ab5216d82
28	T_{len}	3a553e0fefe3e904d838e8f7f8f2a578ac5ffe16356a292747ae7ff804fa2e48a40b94b993ff00da18e10b836f332ec7
29	U_{c-1}	88ebdaa39905dcd14815feeb4cda60ccfa9af68f9dbdb19a229a3cc7d95382d76dcdb9cc6480d2e85f4f253bd443b195
30	T_{len}	52134d54c94831ddec267ab78f44359d675b333b123148c12912c08922438c63bba4c4cf25ec7767ddc9b187f3016312
31	U_c	8002504d9e944e92a818621b9cf53feeb10d773ee19a8790d83bba551972cbe269185b3c84dc87675f2d1355fa2add03
32	T_{len}	d2111d1957dc7f4f443e18ac13b10a73d6564405f3abcf51f1297adc3b314781d2bc9ff3a130f00082e4a2d2092bbe11
33	mk	05975c63d32d2c33eeb95e81ca55b8d4e7e016ccbe7f377cf3487e43f892ae57f89dde478df5f9bada3a33b220048ecf1c7dba5cd2129032c7ae38d43fceadb5a7b6a3169ac88cbd2e8f2d9b35d3d6a9c163055d43d8c60ea3beb152d6843d97d2111d1957dc7f4f443e18ac13b10a73d6564405f3abcf51f1297adc3b314781d2bc9ff3a130f00082e4a2d2092bbe11

5.4 HMAC-SHA-512의 단계별 참조 구현값

입력	P (문자열)	TTAK0!HellowWorld!SHA2512
	S (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	C (10진수)	2048
	kLen (10진수)	1536

위치	변수	중간값(16진수)
1	len	3
2	r	0
3	T_1	0
4	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000001
5	U_1	8cdb2a5cfd6ce3ae5f8d7f4fd12c5b3a81fd049cb3667c8717144d9347f4ed00 2ff4e0d4e5e6d33854d69eb429aa7c917ecf0db06abfd8f40daee412e45378eb
6	T_1	8cdb2a5cfd6ce3ae5f8d7f4fd12c5b3a81fd049cb3667c8717144d9347f4ed00 2ff4e0d4e5e6d33854d69eb429aa7c917ecf0db06abfd8f40daee412e45378eb
7	U_2	f86e761bb5d726063b80085b38a61190b1dc20097c4f7c4411480fd0004e75ed 016121ad31b928aa8d406010189205c7f2b45ff2cebe748829008cb6e8b543e2
8	T_1	74b55c4748bbc5a8640d7714e98a4aaa30212495cf2900c3065c424347ba98ed 2e95c179d45ffb92d996fea4313879568c7b5242a401ac7c24ae68a40ce63b09
9	U_{c-1}	607eec372452367e70d4166b922da9d195087711bd2eeeccc3534de089e541e7 65a1c2f5b921a73997bc31739ce7ba7246e12b49dde206973d7b060d4f635817
10	T_1	6931492b99de3939e0003ea766bc6e4986777cf54d9d489a8f4e9071d75b0bbf 9d337da6b633f315d5f4ca96061498291d6925d384d539523136e8aa695c26c0
11	U_c	9e1da620574d2115fd7137e7ac5b7cf2df9e1e3f0ea85fe0f4dab5de17d5454a 78d3e39547a0b417c21b22930cbd37aa6ba34b60d18c2b8bc8732821314210e6
12	T_1	f72cef0bce93182c1d710940cae712bb59e962ca4335177a7b9425afc08e4ef5 e5e09e33f193470217efe8050aa9af8376ca6eb3555912d9f945c08b581e3626
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000002
15	U_1	e612bbd6be8e86d654028dc1139085f2a1eada8edb514b357846d8c8d7631b98 1705a3c3c2b42a4f53c5b830630684b2712a9a5eb59b1cbe9f78cec484216a4f
16	T_2	e612bbd6be8e86d654028dc1139085f2a1eada8edb514b357846d8c8d7631b98 1705a3c3c2b42a4f53c5b830630684b2712a9a5eb59b1cbe9f78cec484216a4f
17	U_2	83d9b63de6b90556c66b8e0ee115b47e530585ceffbe6b95649b29b1c1a8b74 d0335ec65ed006c63ebf48bc24f85a2b550bf2da6274b4f65920c2e9ce366657
18	T_2	65cb0deb58378380926903cff285318cf2ef5f4024aaad8c2e0f6a53cb7990ec c736fd059c642c896d7af08c47fede9924216884d7efa848c6580c2d4a170c18
19	U_{c-1}	733c06f66f466add4899558235b4cb8dced7549aec854dd0b2f0e3e1275ba91d e7aa00c3a8b058c55ac9051c4340fe7a46df596bf9bfb77bc1d05b5a5b43d0aa
20	T_2	fb317351b6d050a2d291f0dee883250811b9be75ed67f2a5733e6bcbedca8ce5 6a1a3bd4bfa22ea2912705bbd962bd435c658305674a8406b03ab69c5fe2d820
21	U_c	37cd79aa14a73a92693d4b867a08b3a6d30171bf0cefda159a12342b3da8ec76 39d09e80bd5773359ae3a8406d2b2c8bea350a1fa92365bea2b6f77d9e1ed59c

22	T_2	ccfc0afba2776a30bbacbb58928b96aec2b8cfcae18828b0e92c5fe0d062609353caa55402f55d970bc4adfbb44991c8b650891ace69e1b8128c41e1c1fc0dbc
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	6296f8f7e1420c4dbf7681d91bb06e4cf2e71b7d6f6c5c497c92e6fbcbedb654db87cb4cd878b83c73e16e083e09cb39067570c32e78a1692edee96ffb127dcd
26	T_{len}	6296f8f7e1420c4dbf7681d91bb06e4cf2e71b7d6f6c5c497c92e6fbcbedb654db87cb4cd878b83c73e16e083e09cb39067570c32e78a1692edee96ffb127dcd
27	U_2	27d2abf84726a1f3914e9bcc331e45b5cee6b79d4b3c5f79b9776fdd20ae43ae4d57da1834ac65d918757406511406 0c36b71084cc79967b56faeda8beeea01b
28	T_{len}	4544530fa664adbe2e381a1528ae2bf93c01ace024500330c5e58926eb43f5fa96d01154ecd4dde56b941a0e6f1dcd3530c26047e2013712782404c745fcddd6
29	U_{c-1}	9493a6f9edaf22a15187ecbc2e8ae3329dd225bc07b7987bb26bcef828f5f08adb0d749a9aff90aea97a96d0d7c3e3faca087b79710cbc2a917d539126ff90dd
30	T_{len}	120f16448086869041a899e9444ac779c9af8984e8d29fcd2b6b498ded48f3a6749fc10fd2d67975ac5bc0b7371ea787d5e8b6bb0a205ebf1d0b86994fda73cc
31	U_c	5585efa1d6ff11c27960c4627a64cf27be05f0ca0f23a76b280c367e064d7bc829392b2b63f0af0353437c66d00a96b04d5aff37d51e9e8aa479c5b3d0a3b3cc
32	T_{len}	478af9e55679975238c85d8b3e2e085e77aa794ee7f138a603677ff3eb05886e5da6ea24b126d676ff18bcd1e714313798b2498cdf3ec035b972432a9f79c000
33	mk	f72cef0bce93182c1d710940cae712bb59e962ca4335177a7b9425afc08e4ef5e5e09e33f193470217efe8050aa9af8376ca6eb3555912d9f945c08b581e3626ccfc0afba2776a30bbacbb58928b96aec2b8cfcae18828b0e92c5fe0d062609353caa55402f55d970bc4adfbb44991c8b650891ace69e1b8128c41e1c1fc0dbc478af9e55679975238c85d8b3e2e085e77aa794ee7f138a603677ff3eb05886e5da6ea24b126d676ff18bcd1e714313798b2498cdf3ec035b972432a9f79c000

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 TTAK.KO-12.0xxx-Part1

이 표준에서 제시하는 SHA-2를 사용하는 경우의 참조구현값에 대한 구성, 용어 정의 및 약어를 제시하는 '제1부 일반' 표준임

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] NIST FIPS SP 800-132, “Recommendation for Password-Based Key Derivation – Part 1: Storage Applications”, 2010. 12.

[2] ISO/IEC 10118-3, “Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions”, 2004.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.xx	제정 TTAK.KO-12.0xxx-Part2	-	정보보호기반 (PG501)