TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.xxxx-Part3 제정일: 2018년 12월 xx일

패스워드 기반 키 유도 함수 - 제3부: 해시 함수 LSH

Password-based Key Derivation Function - Part3: Hash Function LSH

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 LSH를 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 LSH를 적용할 경우의 참조 구현 값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 제1부 일반에 규정된 패스워드 기반 키 유도 함수로 TTAK.KO-12.0276에 규정된 해시 함수 LSH를 적용한 결과로, PBKDF와 LSH는 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 LSH about implementation conformance.

2 Summary

The standard specifies the test vectors of PBKDF based on LSH 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 LSH specified in TTAK.KO-12.0276, the PBKDF mechanism specified in Part 1: General. And, PBKDF and LSH conform to the specifications of each standard

목 차

패스워드 기반 키 유도 함수
- 제3부: 해시 함수 LSH
(Password based Key Derivation Function)
- Part3: Hash Function LSH)

1 적용 범위

제1부에서 정의한 패스워드 기반 키 유도 함수는 HMAC을 기반 함수로 사용한다. 이 표준은 HMAC의 기반 해시 함수로 LSH를 적용하는 패스워드 기반 키 유도 함수의 참조 구현값을 제시한다. 참조 구현값 생성에 사용된 해시 함수는 <표 1-3>과 같다.

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

해시 함수	LSH-224 LSH-512-224	LSH-256 LSH-512-256	LSH-384	LSH-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 1-4>와 같다.

<표 1-2> PRF 알고리즘

구분	알고리즘	
의사난수함수 (PRF)	HMAC-LSH	HMAC-LSH-224
		HMAC-LSH-256
		HMAC-LSH-384
		HMAC-LSH-512
		HMAC-LSH-512-224
		HMAC-LSH-512-256

2 인용 표준

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

- TTAK.KO-12.0276, “해시 함수 LSH”, 2015.12.16.

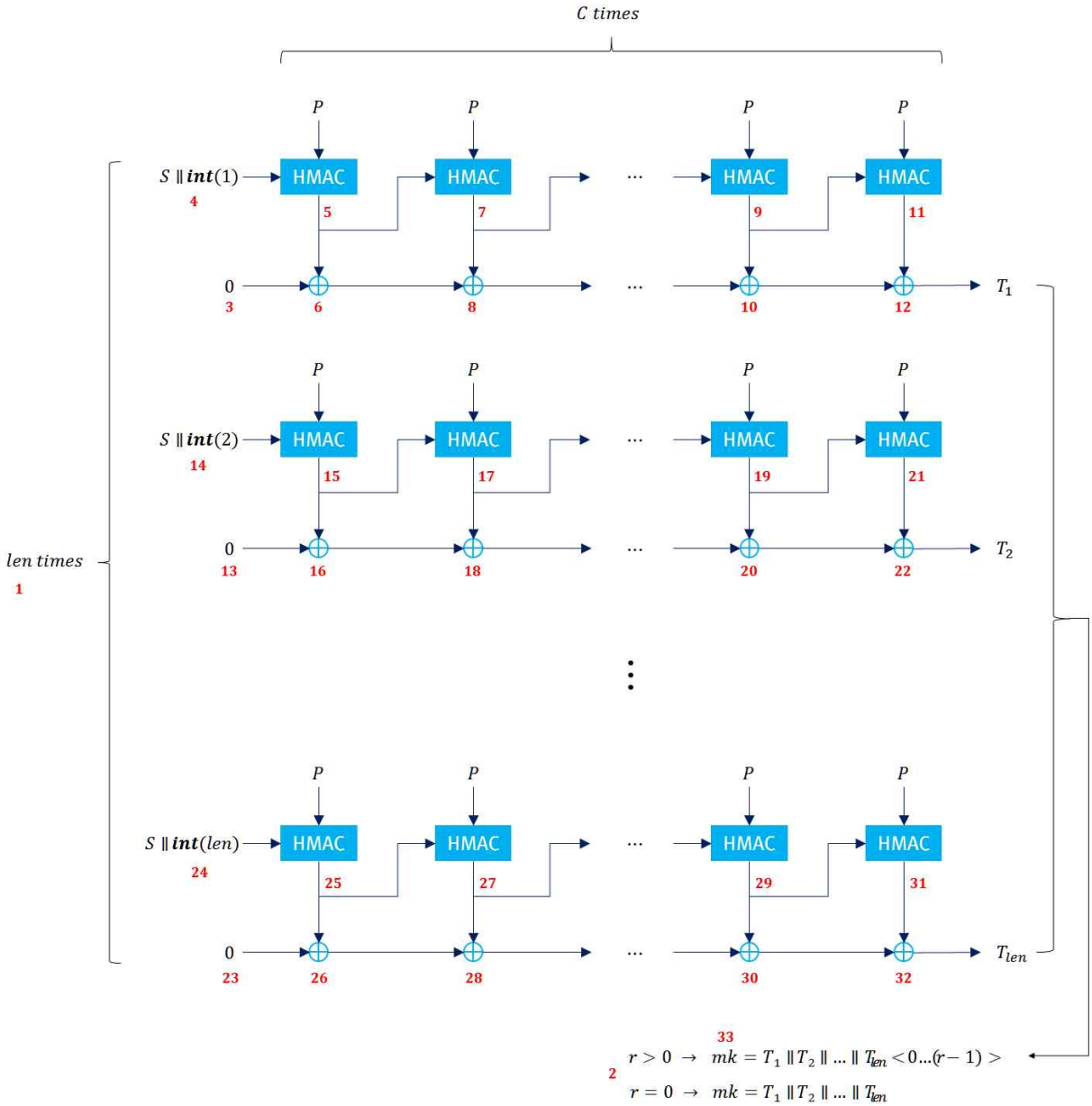
3 용어 정의

- 해당없음

4 약어

- 해당없음

5 참조 구현값


C times
P
S ‖ int(1)
HMAC
4
5
7
9
11
0
3
6
8
10
12
T1
S ‖ int(2)
14
15
17
19
21
13
16
18
20
22
T2
len times
1
S ‖ int(len)
24
25
27
29
31
23
26
28
30
32
Tlen
33
2
r > 0 → mk = T1 ‖ T2 ‖ ... ‖ Tlen < 0...(r − 1) >
r = 0 → mk = T1 ‖ T2 ‖ ... ‖ Tlen

5.1 HMAC-LSH-224의 단계별 참조구현값

입력	P (문자열)	TTAK0!HellowWorld!LSH256224
	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	b42baf5e5cac94428dcf4f39b00a86a32f1b8993a76f85bd08d373a1
6	T_1	b42baf5e5cac94428dcf4f39b00a86a32f1b8993a76f85bd08d373a1
7	U_2	5fcc93a2650398ebf998a0fd13bd17b46ce1f8e28eded2df7e2ff61d
8	T_1	ebe73cfc39af0ca97457efc4a3b7911743fa717129b1576276fc85bc
9	U_{c-1}	9052c6563ce8e826423f4d8ab2eb154b886f732c70d7da0a030a9b8d
10	T_1	d507f050cdd86f45a5ff913925873e26d9493e14f8249372bcfcaf9d
11	U_c	eaebd4d9627bdb3d00c8c84c9ce767c6aff558da1f921ea073047300
12	T_1	3fec2489afa3b478a5375975b96059e076bc66cee7b68dd2cff8dc9d
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000002
15	U_1	196375f9c390552603f78744c0522677377bf6eedad54ff98b5376b2
16	T_2	196375f9c390552603f78744c0522677377bf6eedad54ff98b5376b2
17	U_2	f3155137dcc32a0c59186ba42b0d72757348b214a2b443fc65b97a9c
18	T_2	ea7624ce1f537f2a5aefece0eb5f5402443344fa78610c05eeea0c2e
19	U_{c-1}	70569ff090e5551f9d66e3ad87b4ec4cc86a842e72621fb3548fe7bb
20	T_2	64a3720fdf7876e28021db5c66b09b81410a88dbc266722e0594ca51
21	U_c	ae661bbf2afbfdc9fe207d618eaf01bff155d11993762efe032a4d7a
22	T_2	cac569b0f5838b2b7e01a63de81f9a3eb05f59c251105cd006be872b
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000003
25	U_1	8dbc6ac99bbed1551af70064a9afbfaaf78eae0556d71daa6c586b36
26	T_{len}	8dbc6ac99bbed1551af70064a9afbfaaf78eae0556d71daa6c586b36
27	U_2	c6e705a2da01ebf9bcf379e6d065f2b9a26fff03e4ae0f0e23ca3a33
28	T_{len}	4b5b6f6b41bf3aaca604798279ca4d1355e15106b27912a44f925105
29	U_{c-1}	214c7a6bf343f5e2425a2c28977e7cd2833d846d235092596ecbe20c
30	T_{len}	35a46603a62faf4981df1345f6e34fa22ece44552efe72cc90a4b422
31	U_c	442287312c06e396e3e850d90a540389c63a9a1c7c2462fd07e38fbf
32	T_{len}	7186e1328a294cdf6237439cfcb74c2be8f4de4952da103197473b9d
33	mk	3fec2489afa3b478a5375975b96059e076bc66cee7b68dd2cff8dc9dcac569b0f5838b2b7e01a63de81f9a3eb05f59c251105cd006be872b7186e1328a294cdf6237439cfcb74c2be8f4de4952da103197473b9d

5.2 HMAC-LSH-256의 단계별 참조구현값

입력	P (문자열)	TTAK0!HellowWorld!LSH256256
	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	1042e9a230f4982818c78bb1ace2f648f8529f0213832bdf06ec5fd38deadc08
6	T_1	1042e9a230f4982818c78bb1ace2f648f8529f0213832bdf06ec5fd38deadc08
7	U_2	6233a016e5ee08962b70c05aba0854687f80e9ac7cfc2dded79e27220835f5ba
8	T_1	727149b4d51a90be33b74beb16eaa22087d276ae6f7f0601d17278f185df29b2
9	U_{c-1}	5e650b447acd447db5978b307670a4737de8c74137e233d4d9dbd0f34d468cd7
10	T_1	1dc96f6e57003d2616b5e09d0af4b25406bf02ca552cd7027e166d47b54409c3
11	U_c	18f272bf5d3aaaf392546722e9912725a9caa864c06b1bbafd4fea6100dc78f8
12	T_1	053b1dd10a3a97d584e187bfe3659571af75aaae9547ccb883598726b598713b
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000002
15	U_1	16b71f3c3e6e88eee037ddc4f99cc4530350d612361af5cddcae99a65fd6ee23
16	T_2	16b71f3c3e6e88eee037ddc4f99cc4530350d612361af5cddcae99a65fd6ee23
17	U_2	6079d43aa5ce0dca8d17badeb5e0400ec5d0d5e3b704ca2be22f30278b6c1131
18	T_2	76cecb069ba085246d20671a4c7c845dc68003f1811e3fe63e81a981d4baff12
19	U_{c-1}	84c2cc4b2b4856c4c8031976945b14a38e3196e2dcf4974bdd83b6929eaa4524
20	T_2	b7daaae0f82bfe861113ea8bedd519b13a5afa4d0518c7bbb544806801f3c5e2
21	U_c	a7f2020d084e53f7296f07e8fed1dd9ef04880ebf9565c6702f553b91f79862f
22	T_2	1028a8edf065ad71387ced631304c42fca127aa6fc4e9bdcb7b1d3d11e8a43cd
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	8c09a86dc1240577f733fbd1dcecc97ea574cd798e935c853e2a7362017f2a85
26	T_{len}	8c09a86dc1240577f733fbd1dcecc97ea574cd798e935c853e2a7362017f2a85
27	U_2	f221ada3e4ed51ac52aa8db3eaf7642803f261121e413fb734eb308ddeaa2598
28	T_{len}	7e2805ce25c954dba5997662361bad56a686ac6b90d263320ac143efdfd50f1d
29	U_{c-1}	f39e6488d815ac56f57e859bc95c25e8e1576bc1268f50f60cbdedac2697460a
30	T_{len}	8c61525a348ef77a0493f59e189750375d3ca577c160853ae9c57a70e037b370
31	U_c	17f0a5bc37f8a9743f26cf7296338d54c5ef2bfc879536371f2594f94e458c6d
32	T_{len}	9b91f7e603765e0e3bb53aec8ea4dd6398d38e8b46f5b30df6e0ee89ae723f1d
33	mk	053b1dd10a3a97d584e187bfe3659571af75aaae9547ccb883598726b598713b 1028a8edf065ad71387ced631304c42fca127aa6fc4e9bdcb7b1d3d11e8a43cd 9b91f7e603765e0e3bb53aec8ea4dd6398d38e8b46f5b30df6e0ee89ae723f1d

5.3 HMAC-LSH-384의 단계별 참조구현값

입력	P (문자열)	TTAK0!HellowWorld!LSH512384
	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	b54a43991dfc4f9997b2870bc742ca6ec1f07019e938ec225e5dada8b65f83d4 9db5639481466467f8f07cb83b076baa
6	T_1	b54a43991dfc4f9997b2870bc742ca6ec1f07019e938ec225e5dada8b65f83d4 9db5639481466467f8f07cb83b076baa
7	U_2	63209b8fa57ea2208bcd512ce4672852d69e2ddf295e93ecde096176c75f645f f21a25de89fef220227560bded96bcd6
8	T_1	d66ad816b882edb91c7fd6272325e23c176e5dc6c0667fce8054ccde7100e78b 6faf464a08b89647da851c05d691d77c
9	U_{c-1}	b8ee2e1d78e175e408b89b795dda083fb16f89b4bd54566487581d994e6bc719 b6473dc4b7708ebd943d90ae6c134442
10	T_1	9f657cfe48b01de7d1c8e6d96e2dac24782571fef12b1779c90bc841501da9f8 d03a7cd26fb140a0de8fe08d468b3743
11	U_c	00f847a1b73becf258c17805bc9c6779b66375deee970cda8cb9287132badde7 1e8b6c3c8dabb87ecffb0af7f6622f54
12	T_1	9f9d3b5fff8bf11589099edcd2b1cb5dce4604201fbc1ba345b2e03062a7741f ceb110eee21af8de1174ea7ab0e91817
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00000002
15	U_1	2b4fb11b422b00dc25d7006bcd2db29b22cf26df5d905d177e86e31e81c50025 e88837376037534c755924c4538dc33c
16	T_2	2b4fb11b422b00dc25d7006bcd2db29b22cf26df5d905d177e86e31e81c50025 e88837376037534c755924c4538dc33c
17	U_2	47c4e293b309b4e58514f3991878d57bf2d1e9ffd5c50d47ac814c0b1253da01 09a531c1265f9b7a358e572455d4e704
18	T_2	6c8b5388f122b439a0c3f3f2d55567e0d01ecf2088555050d207af159396da24 e12d06f64668c83640d773e006592438
19	U_{c-1}	9ebdb7276090f410f95fd1a63ea181da916a31db98f5fa44e476a55c11fcdb80 cae36422c2b9f908736b9c4fb020168b
20	T_2	618c4f7911588174a99f6ec7d7c38649c53e3424fb95d1898374125e3e63d763 68cf561e6f63f406963c644f9e276b92
21	U_c	0ade714a87c755597d64f8a3b98295d30e32146b0e3f387bad86f5f9d6dfb635 b3d7efb8ba602a78d907baf594e57f90
22	T_2	6b523e33969fd42dd4fb96646e41139acb0c204ff5aae9f22ef2e7a7e8bc6156 db18b9a6d503de7e4f3bdeba0ac21402

23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	a149c237eb2f859a39c44a49f0d2dd97f9bfe4c4f6d402569d3df87bf5de48298c58f3589995e0ad9ef60b4a82b98cc6
26	T_{len}	a149c237eb2f859a39c44a49f0d2dd97f9bfe4c4f6d402569d3df87bf5de48298c58f3589995e0ad9ef60b4a82b98cc6
27	U_2	72b871c6735439b990c8a526d93c1b0796cafa5dc2456507e8245b7dacfa210e4a22399b23f8bcb86d044db9cb2d2232
28	T_{len}	d3f1b3f1987bbc23a90cef6f29eec6906f751e99349167517519a30659246927c67acac3ba6d5c15f3f246f34994aef4
29	U_{c-1}	3f75b1a1ec40168f70b7f2501087e6bf6222e2db9e86f59e4b308ef4806f5bdb8373940242cca35bbac02d7bff9676f1
30	T_{len}	bb62314e81412a6cf4fc230c228cae43b74d11b3ee2d6b09b75f93ab954264c70bad8ec245855568e257dab57af04b21
31	U_c	f2f9ef4b9a9a6a71e4c99061371af8ac0667ec7d40b56bf328072c084c81153ffad4aa9d742414c1019100ba451fd4ce
32	T_{len}	499bde051bdb401d1035b36d159656efb12afdceae9800fa9f58bfa3d9c371f8f179245f31a141a9e3c6da0f3fef9fef
33	mk	9f9d3b5fff8bf11589099edcd2b1cb5dce4604201fbc1ba345b2e03062a7741fceb110eee21af8de1174ea7ab0e918176b523e33969fd42dd4fb96646e41139acb0c204ff5aae9f22ef2e7a7e8bc6156db18b9a6d503de7e4f3bdeba0ac21402499bde051bdb401d1035b36d159656efb12afdceae9800fa9f58bfa3d9c371f8f179245f31a141a9e3c6da0f3fef9fef

5.4 HMAC-LSH-512의 단계별 참조구현값

입력	P (문자열)	TTAK0!HellowWorld!LSH512512
	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	8646024a7f39c2a6e484803458f10f18892a50743ef2cd2aa8cfbdb3262ca434 6a89346186ab9d94d49d7508c478882f1b62d9fcce4e40ce61e3f507ba35a607
6	T_1	8646024a7f39c2a6e484803458f10f18892a50743ef2cd2aa8cfbdb3262ca434 6a89346186ab9d94d49d7508c478882f1b62d9fcce4e40ce61e3f507ba35a607
7	U_2	870b736b7047e84b70048f9a4ff4f4098ae050c65e4bc9c14aee5310c00872a8 d29d89f3db54e3834c789e478e604bf6a4bfffaf1985a4722aa069377ddc27e5
8	T_1	014d71210f7e2aed94800fae1705fb1103ca00b260b904ebe221eea3e624d69c b814bd925dff7e1798e5eb4f4a18c3d9bfdd2653d7cbe4bc4b439c30c7e981e2
9	U_{c-1}	621b468da49f6c4f7b3e5e8f78ad46c25cdda4473c098d98b850e4f05c3531ba 0bbb6f9c2386e3769723f9dfc725d6e3e9c4be1c3923cf7cd993553de1abc35b
10	T_1	234ce10731cf8e9bbab26e302b17e461477be805eb3436416e29a95c38c85db5 0231b36c107a465574d04ed893fe2250923a0e6576ce0184f1c3a9274d1add0b
11	U_c	c6ea6fe83437803e66b971d98b7b020ca797bd0d4652dd7b4e1d99e1c54a35ab 883321d5f016dc1ac00fc94298abf90435e565a4cc66c4dc89391f323d5497f9
12	T_1	e5a68eef05f80ea5dc0b1fe9a06ce66de0ec5508ad66eb3a203430bdfd82681e 8a0292b9e06c9a4fb4df879a0b55db54a7df6bc1baa8c55878fab615704e4af2
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000002
15	U_1	170b49450431d537d169dbfadd8a8c09b68a2c187192b0a8979b46237deb73b7 88f03de23874042300299da838f4d6c4edc9032c8d9c4d3ba8956e66bc898278
16	T_2	170b49450431d537d169dbfadd8a8c09b68a2c187192b0a8979b46237deb73b7 88f03de23874042300299da838f4d6c4edc9032c8d9c4d3ba8956e66bc898278
17	U_2	112824085e628c2bf569d362d2aeb3982611afc8e1472b2d298b0f9919116302 9f380aa3342cf863447e0cd39c146da0044e03d7e7d8f5397bd7df60c2aea4d8
18	T_2	06236d4d5a53591c240008980f243f91909b83d090d59b85be1049ba64fa10b5 17c837410c58fc404457917ba4e0bb64e98700fb6a44b802d342b1067e2726a0
19	U_{c-1}	ea10d8f211854631eff260221bd5faedd6294448d4662e97e9fbfa48a96e5471 a319a2d3063797310d9a8bf01c23e5963c502d5ff44ceadd09d26ff29a66b9b5
20	T_2	1c60edac8ae970d75cdcce610646a217c6352ab2872182adab165f10cefea20f 1a654e7041e7fbe83eb3a12584743b0324a5f0d08327ec0d7412bc19c718ba93
21	U_c	c64d63128c58221504834737d722e714e194d2b6e0cc501af0c45e9e120c9c7e 84d7320d4b806b74833ec9093d507fb20c29d15bea48d96fe15ee1709368c649

22	T_2	da2d8ebe06b152c2585f8956d164450327a1f80467edd2b75bd2018edcf23e719eb27c7d0a67909cbd8d682cb92444b1288c218b696f3562954c5d6954707cda
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	2af0fda2d23a86327ce86f579c3e721682afdf782a8ab315f0feb681a00fa69479cc3b0b9c609574d08b9bd4a15a988e19a01d60ec1ec98060d1b10a12ee2934
26	T_{len}	2af0fda2d23a86327ce86f579c3e721682afdf782a8ab315f0feb681a00fa69479cc3b0b9c609574d08b9bd4a15a988e19a01d60ec1ec98060d1b10a12ee2934
27	U_2	dfe9e5c9b1df37ce6400dfd030c0834f43acc04d80b2fa2f84fee6c3548894610f5bc7cf4032d7d69a9b11c7088a5c4e442a592d8dd4c18abf26bd8a10403de8
28	T_{len}	f519186b63e5b1fc18e8b087acfef159c1031f35aa38493a74005042f48732f57697fcc4dc5242a24a108a13a9d0c4c05d8a444d61ca080adff70c8002ae14dc
29	U_{c-1}	d71b9496e589b345201992d21bf92ac8c4899c28873f755bf297227e7728d58a754f6fafb9a37b089b82ea202a87cb2c803e0cdaae906c7964c9adea5b4ed61c
30	T_{len}	12a005fd897c159b122a410acacaf10dd1134faf039a8c81f9012b9f191084a9875831736ebe77e175434b5a59b147677108439aad0b7b58fabbd8d3077e046a
31	U_c	9fa84debfb25a6ec85ea0fdd9a4029a054a48269f2d8b0051516283d7e46fe98df35a0b30738f2c12e54b9d2a87fd461a52bbe22466b42a711e04dbca138d6eb
32	T_{len}	8d0848167259b37797c04ed7508ad8ad85b7cdc6f1423c84ec1703a267567a31586d91c0698685205b17f288f1ce9306d423fdb8eb6039ffeb5b956fa646d281
33	mk	e5a68eef05f80ea5dc0b1fe9a06ce66de0ec5508ad66eb3a203430bdfd82681e8a0292b9e06c9a4fb4df879a0b55db54a7df6bc1baa8c55878fab615704e4af2da2d8ebe06b152c2585f8956d164450327a1f80467edd2b75bd2018edcf23e719eb27c7d0a67909cbd8d682cb92444b1288c218b696f3562954c5d6954707cda8d0848167259b37797c04ed7508ad8ad85b7cdc6f1423c84ec1703a267567a31586d91c0698685205b17f288f1ce9306d423fdb8eb6039ffeb5b956fa646d281

5.5 HMAC-LSH-512-224의 단계별 참조구현값

입력	P (문자열)	TTAK0!HellowWorld!LSH512224
	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	86004b86cdd0fdd720f29e096adb3e8586be90028a06b83247ea861a
6	T_1	86004b86cdd0fdd720f29e096adb3e8586be90028a06b83247ea861a
7	U_2	79276fad1ae3fc4264a8a393beecb6ee09fb6830c08feedd944d0268
8	T_1	ff27242bd7330195445a3d9ad437886b8f45f8324a8956efd3a78472
9	U_{c-1}	80f961180fd47e5d067702d83b9aa31dd15897bce35c94f6ede31b9f
10	T_1	343c1698a366b7ae5e5ffed860573e24fdd7dd5fbe018d8d8fc4ac06
11	U_c	51858bd2fbe9c1b50d155fb4f2470fefc6e8969f6710c23e8b205953
12	T_1	65b99d4a588f761b534aa16c921031cb3b3f4bc0d9114fb304e4f555
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000002
15	U_1	a071b504cff7a337086eae23a116a8c090ea106e4532a2bb6a9c8151
16	T_2	a071b504cff7a337086eae23a116a8c090ea106e4532a2bb6a9c8151
17	U_2	e347554e90185be8c493fcd2c5bb22c873e27c220aa316d63696e1ff
18	T_2	4336e04a5feff8dfccfd52f164ad8a08e3086c4c4f91b46d5c0a60ae
19	U_{c-1}	e087755724f0591562b6633792de794b9a9cfdef20574bc6010515bf
20	T_2	ea74f51c67a76104bfa914f503ddca6f6c34310fd66be6796aafb764
21	U_c	11b5abcf133888a7e7210974bd37b7d7cd89269b8a78091d6f3c440d
22	T_2	fbc15ed3749fe9a358881d81beea7db8a1bd17945c13ef640593f369
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabb00000003
25	U_1	ec6a91eedfcdbe20936331d15286bc3561cf9fd2dd46f5a3b5e2380f
26	T_{len}	ec6a91eedfcdbe20936331d15286bc3561cf9fd2dd46f5a3b5e2380f
27	U_2	411a35e3600752ba515c2fec2a12a80453ec728abcd6b62d85df0edd
28	T_{len}	ad70a40dbfcaec9ac23f1e3d789414313223ed586190438e303d36d2
29	U_{c-1}	1fc0a2d9e39e5e530ac443ec46520644ced77bbd0c74abd1d0873b25
30	T_{len}	3eb193f2c4c417f3aca04e969663ab60cf866d99b06915ec51ecc41d
31	U_c	6c1d79106b607b38fe132b2cc0d4ddb3eddf695eca86add33c957785
32	T_{len}	52aceae2afa46ccb52b365ba56b776d3225904c77aefb83f6d79b398
33	mk	65b99d4a588f761b534aa16c921031cb3b3f4bc0d9114fb304e4f555fbc15ed3749fe9a358881d81beea7db8a1bd17945c13ef640593f36952aceae2afa46ccb52b365ba56b776d3225904c77aefb83f6d79b398

5.6 HMAC-LSH-512-256의 단계별 참조구현값

입력	P (문자열)	TTAK0!HellowWorld!LSH512256
	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	e47b2c237d3beb73581dd2b373993949a78f5b351f5b5da9f65ef2669cc6dadc
6	T_1	e47b2c237d3beb73581dd2b373993949a78f5b351f5b5da9f65ef2669cc6dadc
7	U_2	e9ee8a40b70b6f006c9a510a7d07022b27e55e9e9a624ac674eca0dec2e37ff2
8	T_1	0d95a663ca308473348783b90e9e3b62806a05ab8539176f82b252b85e25a52e
9	U_{c-1}	e0c32d4f518e9ec05075b093a90c18b52b7750ef30871f20e7a55c8245379199
10	T_1	f39c97008536c481ea471ab15721bf60d074ed70b1972a1586e4455141434edc
11	U_c	400dfc2c373de66731e4a9d97e79e4f3f1257576ef0ba779c92c2354369e1420
12	T_1	b3916b2cb20b22e6dba3b36829585b93215198065e9c8d6c4fc8660577dd5afc
13	T_2	0
14	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000002
15	U_1	9fc56e8f0b2aaec66663bdc214e85bc8f6c2f3ab19be50783e758991f690a3a2
16	T_2	9fc56e8f0b2aaec66663bdc214e85bc8f6c2f3ab19be50783e758991f690a3a2
17	U_2	cdc76ebbf0ffc6b5752985643d10571935acf4a1e3b8014b09e55b8070ec162d
18	T_2	52020034fbd56873134a38a629f80cd1c36e070afa0651333790d211867cb58f
19	U_{c-1}	b20d236965dc6c770ca3b8a5c1f1470812dcb982ad44ab7b337e8d76898e6c4b
20	T_2	4a8099fd19109e539322b7a7cb6bcd0a596a2a6e994773f6508a4f4c10e009a4
21	U_c	e0e81d8f83eeee0a59d6bdf882bb31d3e6f775054eef2a40809a630c5f70ad48
22	T_2	aa6884729afe7059caf40a5f49d0fcd9bf9d5f6bd7a859b6d0102c404f90a4ec
23	T_{len}	0
24	U_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00000003
25	U_1	572f10112849e558b179ce7a6f407a062579fcc83b6c8b636dde25485eee8369
26	T_{len}	572f10112849e558b179ce7a6f407a062579fcc83b6c8b636dde25485eee8369
27	U_2	ff4e0ab071dd9e9580fe8504958974abee5ab1c63a042d72360aa1c3814fed4e
28	T_{len}	a8611aa159947bcd31874b7efac90eadcb234d0e0168a6115bd4848bdfa16e27
29	U_{c-1}	382133cb64cc70fa3f528a6a76d45b9128cb1742dfcb1d92193a82ed16c041dd
30	T_{len}	487f6313bad5fcd6b133f844b660227a1cae27dcadbc6a7361b7bba44062e958
31	U_c	e836f1074835377218cfa051fcd5fceb7e95bf49d930bf331ab3fe783c429374
32	T_{len}	a0499214f2e0cba4a9fc58154ab5de91623b9895748cd5407b0445dc7c207a2c
33	mk	b3916b2cb20b22e6dba3b36829585b93215198065e9c8d6c4fc8660577dd5afc aa6884729afe7059caf40a5f49d0fcd9bf9d5f6bd7a859b6d0102c404f90a4ec a0499214f2e0cba4a9fc58154ab5de91623b9895748cd5407b0445dc7c207a2c

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 LSH를 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.

※ 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-Part3	-	정보보호기반 (PG501)