TTA Standard

정보통신단체표준(국문표준)

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

HMAC 기반 키 유도 함수
- 제3부: 해시 함수 LSH

HMAC based Key Derivation Functions
- Part3: Hash Function LSH

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 HMAC 기반 키 유도 함수에 해시 함수 LSH를 적용할 경우의 참조 구현값을 제시하여, 키 유도 함수의 구현 정확성을 확인할 수 있도록 한다.

2 주요 내용 요약

이 표준은 HMAC을 의사난수함수(PRF)로 사용하는 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 기반 키 유도 함수로 TTAK.KO-12.0276에 규정된 해시 함수 LSH를 적용한 결과로, KDF와 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 HMAC based on LSH about implementation conformance.

2 Summary

The standard specifies the test vectors of KDF used as HMAC(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 as HMAC(LSH), the KDF based on HMAC mechanism specified in Part 1: General.
And, KDF and LSH conform to the specifications of each standard.

목 차

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

1 적용 범위

이 표준은 제1부 일반에서 정의한 HMAC 기반 키 유도 함수를 해시 함수 LSH로 구현할 경우 활용할 수 있는 참조 구현값을 제시한다. 참조 구현값 생성에 사용된 해시 함수는 <표 1-1>과 같다.

<표 1-1> HMAC 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 1-2>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

또한, HMAC 기반 키 유도함수는 모드에 따라 다른 동작 절차를 따른다. 이러한 모드의 특징을 고려하여 설정한 참조 구현값 생성 시나리오를 정리하면 <표 1-3>와 같다.

<표 1-3> 모드에 따른 시험 분류

구분		HMAC
(5절) 카운터 모드를 이용한 키 유도 함수 참조 구현값	5.1	HMAC-LSH-224
	5.2	HMAC-LSH-256
	5.3	HMAC-LSH-384
	5.4	HMAC-LSH-512
	5.5	HMAC-LSH-512-224
	5.6	HMAC-LSH-512-256
(6절) 피드백 모드를 이용한 키 유도 함수 참조 구현값	6.1	HMAC-LSH-224
	6.2	HMAC-LSH-256
	6.3	HMAC-LSH-384
	6.4	HMAC-LSH-512
	6.5	HMAC-LSH-512-224
	6.6	HMAC-LSH-512-256
(7절) 더블-파이프라인 반복 모드를 이용한 키 유도 함수 참조 구현값	7.1	HMAC-LSH-224
	7.2	HMAC-LSH-256
	7.3	HMAC-LSH-384
	7.4	HMAC-LSH-512
	7.5	HMAC-LSH-512-224
	7.6	HMAC-LSH-512-256

2 인용 표준

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

3 용어 정의

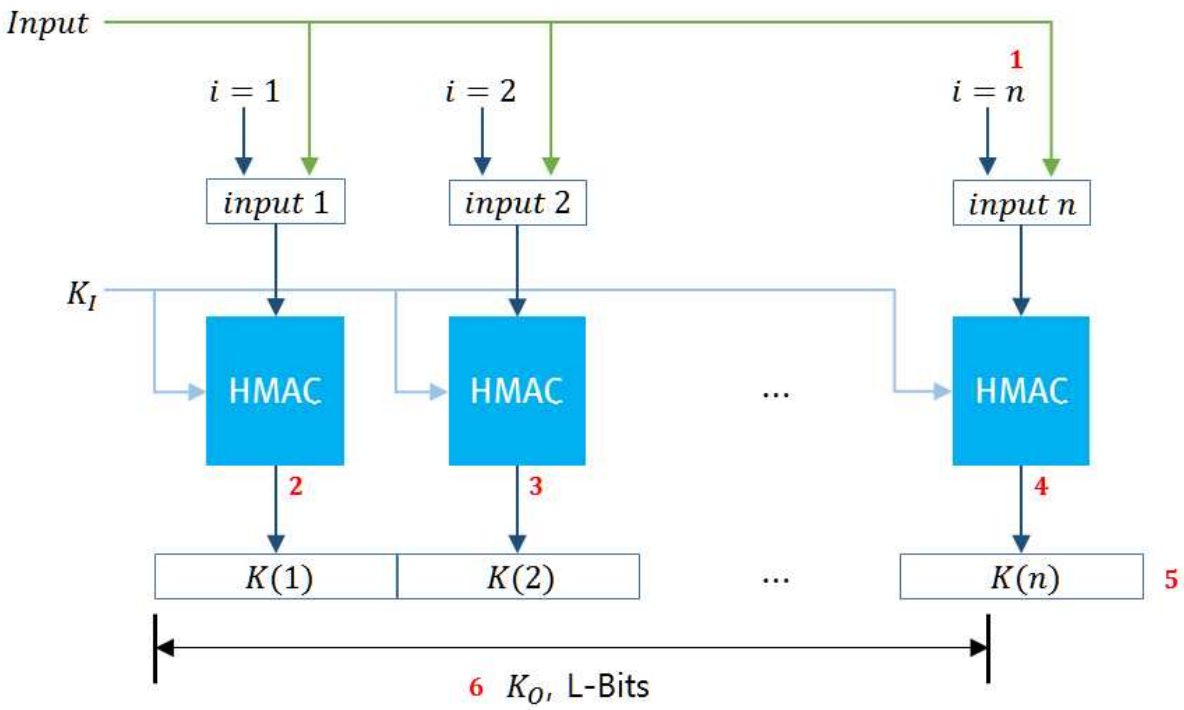
- 해당없음

4 약어

- 해당없음

5 카운터 모드를 이용한 키 유도 함수 참조 구현값

※ $Input = Label \,||\, 0x00 \,||\, Context \,||\, [L]_2$



5.1 HMAC-LSH-224의 단계별 참조 구현값

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	811de5a502f18dfd6443bc0923d7d306f389ef0b2767c649642ae3ec
3	K(2)	a42e0a0a4f74cc4b1065e98da0e550cb90051d274c5fbf8e661bde80
4	K(n)	c9a134a67c1afc4b2821324c355e446d8c771e9c1fcc1d68f57d539b
5	result(n)	811de5a502f18dfd6443bc0923d7d306f389ef0b2767c649642ae3eca42e0a0a 4f74cc4b1065e98da0e550cb90051d274c5fbf8e661bde80c9a134a67c1afc4b 2821324c355e446d8c771e9c1fcc1d68f57d539b
6	K0	811de5a502f18dfd6443bc0923d7d306f389ef0b2767c649642ae3eca42e0a0a 4f74cc4b1065e98da0e550cb90051d274c5fbf8e661bde80c9a134a67c1afc4b 2821324c355e

5.2 HMAC-LSH-256의 단계별 참조 구현값

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	285d66835bc7be45203f66bf71940dee35fd01a06bafebe9c97e229436254517
3	K(2)	4aa4c435b37d6970c3ff23ba815ef0105d697dc0e239e3850f770c3140d51b9e
4	K(n)	cfa1d577875cd30ff7f146dde651fb8912cef8e5226ae18fc62dead0ace3171a
5	result(n)	285d66835bc7be45203f66bf71940dee35fd01a06bafebe9c97e229436254517 4aa4c435b37d6970c3ff23ba815ef0105d697dc0e239e3850f770c3140d51b9e cfa1d577875cd30ff7f146dde651fb8912cef8e5226ae18fc62dead0ace3171a
6	K0	285d66835bc7be45203f66bf71940dee35fd01a06bafebe9c97e229436254517 4aa4c435b37d6970c3ff23ba815ef0105d697dc0e239e3850f770c3140d51b9e cfa1d577875cd30ff7f146dde651fb89

5.3 HMAC-LSH-384의 단계별 참조 구현값

고정된 값	h (16진수)	0180
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	4db27290f3b1e3ef159394dd6a7f0c4362581354353ccbcdaa6f596ad74d64140c9a5116a0d3f54c1ec0fa9ed12142be
3	K(2)	b6eec6790a579e1960a212b11d3f5eb7eff2db346c2e5862d94331a2c0e11f5b4647c0332b2730749e65f2712af26e02
4	K(n)	5a81dfd5092818bef5c44fa1460c7a257687a19a7e200ef973cbf652d8db69535c95a9ebf318ad2e240c91bb00b73265
5	result(n)	4db27290f3b1e3ef159394dd6a7f0c4362581354353ccbcdaa6f596ad74d64140c9a5116a0d3f54c1ec0fa9ed12142beb6eec6790a579e1960a212b11d3f5eb7eff2db346c2e5862d94331a2c0e11f5b4647c0332b2730749e65f2712af26e025a81dfd5092818bef5c44fa1460c7a257687a19a7e200ef973cbf652d8db69535c95a9ebf318ad2e240c91bb00b73265
6	K0	4db27290f3b1e3ef159394dd6a7f0c4362581354353ccbcdaa6f596ad74d64140c9a5116a0d3f54c1ec0fa9ed12142beb6eec6790a579e1960a212b11d3f5eb7eff2db346c2e5862d94331a2c0e11f5b4647c0332b2730749e65f2712af26e025a81dfd5092818bef5c44fa1460c7a257687a19a7e200ef9

5.4 HMAC-LSH-512의 단계별 참조 구현값

고정된 값	h (16진수)	0200
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	7a0e5322cb5722d7260789d1db23f091ac567b002f8b38f3808f53394d73a783 48593b5583374185389ad89f61507061884e89bedeef5670fd868bb5d721a139
3	K(2)	364ac7755100812eb1940fe01458c023ac073a9cf50c30fbfeffd67d33343f0f da1580dd58be4bd234be80600f7062378037678334e0765b139b778656062d8c
4	K(n)	cb02ad4333d8a816a2e9a4a62bc4ea314aa398000a4a357e3a0bd7347edaaa55 075689a7cffe80332b3ec7a548894ac176cdc7935161e600a0893407c3525a72
5	result(n)	7a0e5322cb5722d7260789d1db23f091ac567b002f8b38f3808f53394d73a783 48593b5583374185389ad89f61507061884e89bedeef5670fd868bb5d721a139 364ac7755100812eb1940fe01458c023ac073a9cf50c30fbfeffd67d33343f0f da1580dd58be4bd234be80600f7062378037678334e0765b139b778656062d8c cb02ad4333d8a816a2e9a4a62bc4ea314aa398000a4a357e3a0bd7347edaaa55 075689a7cffe80332b3ec7a548894ac176cdc7935161e600a0893407c3525a72
6	K0	7a0e5322cb5722d7260789d1db23f091ac567b002f8b38f3808f53394d73a783 48593b5583374185389ad89f61507061884e89bedeef5670fd868bb5d721a139 364ac7755100812eb1940fe01458c023ac073a9cf50c30fbfeffd67d33343f0f da1580dd58be4bd234be80600f7062378037678334e0765b139b778656062d8c cb02ad4333d8a816a2e9a4a62bc4ea314aa398000a4a357e3a0bd7347edaaa55

5.5 HMAC-LSH-512-224의 단계별 참조 구현값

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

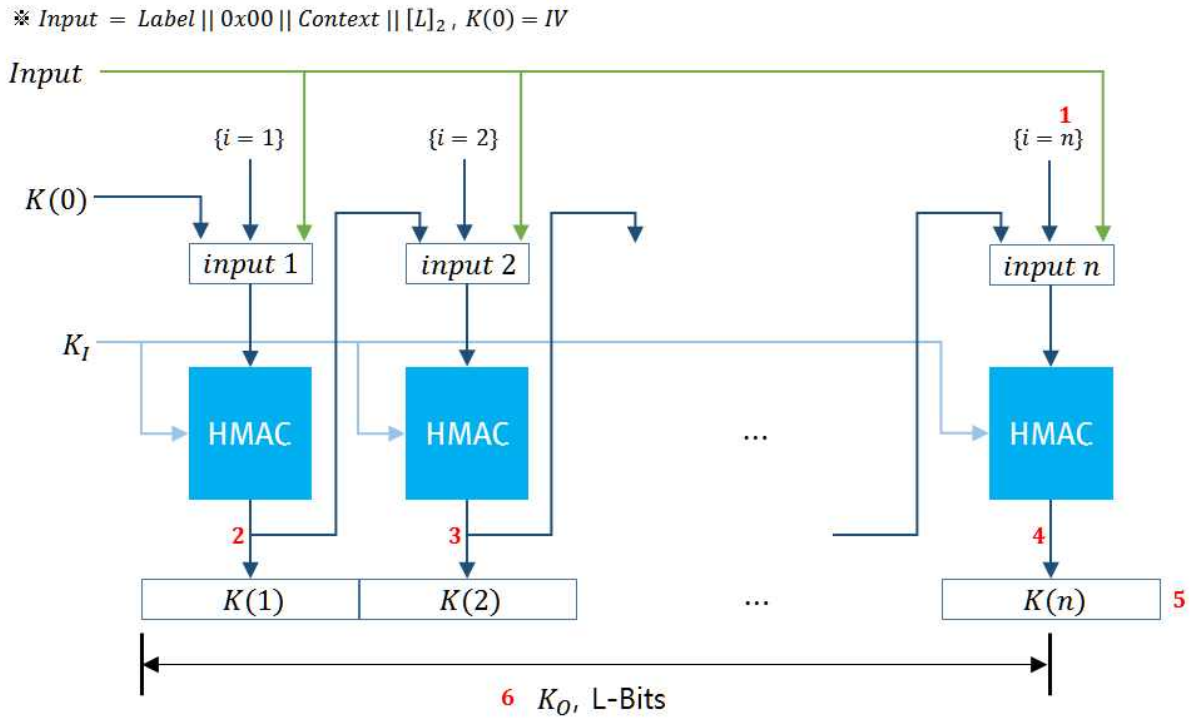
위치	변수	중간값(16진수)
1	n	3
2	K(1)	f30a6558d356497683dba43b72619a68486ce67a316acca03132b58b
3	K(2)	26f49b441cee93489ef9a99d02ef73cebbfe27a53440bbf51d8bee95
4	K(n)	5e592c9d7816b70c33eb207d2303edb2dfdf87ad15b10cdacfa6329d
5	result(n)	f30a6558d356497683dba43b72619a68486ce67a316acca03132b58b26f49b44 1cee93489ef9a99d02ef73cebbfe27a53440bbf51d8bee955e592c9d7816b70c 33eb207d2303edb2dfdf87ad15b10cdacfa6329d
6	K0	f30a6558d356497683dba43b72619a68486ce67a316acca03132b58b26f49b44 1cee93489ef9a99d02ef73cebbfe27a53440bbf51d8bee955e592c9d7816b70c 33eb207d2303

5.6 HMAC-LSH-512-256의 단계별 참조 구현값

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	c6e40f6d7784f8940d108d72f8845d169c1d15c88ca393b901d2afa72fcee813
3	K(2)	2a32b763866282ac570b9402e5d04dd81c0914c0b4c59128722adc2fe6a680cd
4	K(n)	fa766201d98a02841389a2ac29c163e6e4534f9a857413cd7817f5ab482e52fb
5	result(n)	c6e40f6d7784f8940d108d72f8845d169c1d15c88ca393b901d2afa72fcee813 2a32b763866282ac570b9402e5d04dd81c0914c0b4c59128722adc2fe6a680cd fa766201d98a02841389a2ac29c163e6e4534f9a857413cd7817f5ab482e52fb
6	K0	c6e40f6d7784f8940d108d72f8845d169c1d15c88ca393b901d2afa72fcee813 2a32b763866282ac570b9402e5d04dd81c0914c0b4c59128722adc2fe6a680cd fa766201d98a02841389a2ac29c163e6

6 피드백 모드를 이용한 키 유도 함수 참조 구현값



6.1 HMAC-LSH-224의 단계별 참조 구현값

6.1.1 카운터 입력을 사용하고 IV ≠ ∅는 경우

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	a4e08512f46dd9094b0c4d0603233cf9371dae42c0b89b9911cea833
3	K(2)	effb338d12699d7cae883d317958ead3abfe98444d1e7ba3c48f8e29
4	K(n)	f43a2ce9a5d6ccd6c5319f3ed9965dfee9528a17fb327478f9ba3449
5	result(n)	a4e08512f46dd9094b0c4d0603233cf9371dae42c0b89b9911cea833effb338d 12699d7cae883d317958ead3abfe98444d1e7ba3c48f8e29f43a2ce9a5d6ccd6 c5319f3ed9965dfee9528a17fb327478f9ba3449
6	K0	a4e08512f46dd9094b0c4d0603233cf9371dae42c0b89b9911cea833effb338d 12699d7cae883d317958ead3abfe98444d1e7ba3c48f8e29f43a2ce9a5d6ccd6 c5319f3ed996

6.1.2 카운터 입력을 사용하고 IV = ∅인 경우

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	811de5a502f18dfd6443bc0923d7d306f389ef0b2767c649642ae3ec
3	K(2)	fbd497760a9d4611c645c26bd0c047deb25a410eebe74567c3e47b3b
4	K(n)	e7e6fb6432a31566d0423b82cd1e837b7a3d5d7acc423edc6ac78bf1
5	result(n)	811de5a502f18dfd6443bc0923d7d306f389ef0b2767c649642ae3ecfbd49776 0a9d4611c645c26bd0c047deb25a410eebe74567c3e47b3be7e6fb6432a31566 d0423b82cd1e837b7a3d5d7acc423edc6ac78bf1
6	K0	811de5a502f18dfd6443bc0923d7d306f389ef0b2767c649642ae3ecfbd49776 0a9d4611c645c26bd0c047deb25a410eebe74567c3e47b3be7e6fb6432a31566 d0423b82cd1e

6.1.3 카운터 입력을 사용하지 않고 IV ≠ ∅는 경우

고정된 값	h (16진수)	00e0
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	511d89f3f530d081529dd5126c6d4500803f73d47ef57056b7ec6c59
3	K(2)	1bf8a44ffbf1e8403cd7f2553f8f4fcf0f7abd46b19d649c3de4fcbc
4	K(n)	f0d1f2450494d10a45a0d3fbab06ad55366172e6989a97583f02dc25
5	result(n)	511d89f3f530d081529dd5126c6d4500803f73d47ef57056b7ec6c591bf8a44f fbf1e8403cd7f2553f8f4fcf0f7abd46b19d649c3de4fcbcf0d1f2450494d10a 45a0d3fbab06ad55366172e6989a97583f02dc25
6	K0	511d89f3f530d081529dd5126c6d4500803f73d47ef57056b7ec6c591bf8a44f fbf1e8403cd7f2553f8f4fcf0f7abd46b19d649c3de4fcbcf0d1f2450494d10a 45a0d3fbab06

6.1.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

고정된 값	h (16진수)	00e0
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	7c08b0cb988cad74ada55df498f4443c1f2b178be01163a86d97a6e2
3	K(2)	efb1815b843a887018467f0096c91d51949e86942610d82ad0d8ed27
4	K(n)	2be0161109a386c6be04ef248cf35f27e83a9d09e3f69d56262f07b8
5	result(n)	7c08b0cb988cad74ada55df498f4443c1f2b178be01163a86d97a6e2efb1815b843a887018467f0096c91d51949e86942610d82ad0d8ed272be0161109a386c6be04ef248cf35f27e83a9d09e3f69d56262f07b8
6	K0	7c08b0cb988cad74ada55df498f4443c1f2b178be01163a86d97a6e2efb1815b843a887018467f0096c91d51949e86942610d82ad0d8ed272be0161109a386c6be04ef248cf3

6.2 HMAC-LSH-256의 단계별 참조 구현값

6.2.1 카운터 입력을 사용하고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	e76bd339469b024c03609add3f83885f96ceeb72a32d646af546acad9518c58a
3	K(2)	76cd6bf9116ec4a956dc5a6c387bdfdaedc53c0e8370f7dc77ae8cce3cd081f1
4	K(n)	5e10063b679a6ac3d7a5bdd6480faff31087f48ae8a1d005a5ffa2a86dab9ee9
5	result(n)	e76bd339469b024c03609add3f83885f96ceeb72a32d646af546acad9518c58a 76cd6bf9116ec4a956dc5a6c387bdfdaedc53c0e8370f7dc77ae8cce3cd081f1 5e10063b679a6ac3d7a5bdd6480faff31087f48ae8a1d005a5ffa2a86dab9ee9
6	K0	e76bd339469b024c03609add3f83885f96ceeb72a32d646af546acad9518c58a 76cd6bf9116ec4a956dc5a6c387bdfdaedc53c0e8370f7dc77ae8cce3cd081f1 5e10063b679a6ac3d7a5bdd6480faff3

6.2.2 카운터 입력을 사용하고 IV = ∅인 경우

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	285d66835bc7be45203f66bf71940dee35fd01a06bafebe9c97e229436254517
3	K(2)	1fa87ecc56996b2ac77c7d7d0c7cac326b7ab7cb702f95ff75cd1e25f0be2c2f
4	K(n)	5a638260bd6aea517bbf89423b0254848da931d2e697362fc1a0b2122f9899df
5	result(n)	285d66835bc7be45203f66bf71940dee35fd01a06bafebe9c97e229436254517 1fa87ecc56996b2ac77c7d7d0c7cac326b7ab7cb702f95ff75cd1e25f0be2c2f 5a638260bd6aea517bbf89423b0254848da931d2e697362fc1a0b2122f9899df
6	K0	285d66835bc7be45203f66bf71940dee35fd01a06bafebe9c97e229436254517 1fa87ecc56996b2ac77c7d7d0c7cac326b7ab7cb702f95ff75cd1e25f0be2c2f 5a638260bd6aea517bbf89423b025484

6.2.3 카운터 입력을 사용하지 않고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0100
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	df4c8242b575cf800a7cba89f20cfcee15441284c511e10b2597e79bb7cdc870
3	K(2)	0f5be97ece3d57af317c00c951099ac77f3e2b695a079f40b9d72049421e9ddf
4	K(n)	79357d2b405ad4dff1b4d8418635fddc75e8838dca3f32b6b23c55ece7cc47c3
5	result(n)	df4c8242b575cf800a7cba89f20cfcee15441284c511e10b2597e79bb7cdc870 0f5be97ece3d57af317c00c951099ac77f3e2b695a079f40b9d72049421e9ddf 79357d2b405ad4dff1b4d8418635fddc75e8838dca3f32b6b23c55ece7cc47c3
6	K0	df4c8242b575cf800a7cba89f20cfcee15441284c511e10b2597e79bb7cdc870 0f5be97ece3d57af317c00c951099ac77f3e2b695a079f40b9d72049421e9ddf 79357d2b405ad4dff1b4d8418635fddc

6.2.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

고정된 값	h (16진수)	0100
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	5ebb4e14afaa8db0402221f9165ff6f2ed7d20c25a679b84d1013ba5695fea24
3	K(2)	1fc82ad177800890ec778860b02c362c49751292bf32dc739b77bc8bc76cf5a3
4	K(n)	c8e577f8fec1e422a127bf888f9ad4bb1c6b90a40a1cc1e16adbdae7a43b7c40
5	result(n)	5ebb4e14afaa8db0402221f9165ff6f2ed7d20c25a679b84d1013ba5695fea24 1fc82ad177800890ec778860b02c362c49751292bf32dc739b77bc8bc76cf5a3 c8e577f8fec1e422a127bf888f9ad4bb1c6b90a40a1cc1e16adbdae7a43b7c40
6	K0	5ebb4e14afaa8db0402221f9165ff6f2ed7d20c25a679b84d1013ba5695fea24 1fc82ad177800890ec778860b02c362c49751292bf32dc739b77bc8bc76cf5a3 c8e577f8fec1e422a127bf888f9ad4bb

6.3 HMAC-LSH-384의 단계별 참조 구현값

6.3.1 카운터 입력을 사용하고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0180
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	b44e3c56dff45afb56fff474dece853816f5c5577aa18996b73a1f970e01b09fa12d193fa98a70456f431360d6948e26
3	K(2)	a2ea94ff52b66ac71c03ab8ee5611b107d7a52366737184d97a1e9a39b802cce551166e7861b1834c0f2936302ec9110
4	K(n)	8dcfe9c66afa2555fd41cce8b3c57e66db92804590c4b6758a0acde49021cff5e7951e1d9c0c2f70e07807a5f059021f
5	result(n)	b44e3c56dff45afb56fff474dece853816f5c5577aa18996b73a1f970e01b09fa12d193fa98a70456f431360d6948e26a2ea94ff52b66ac71c03ab8ee5611b107d7a52366737184d97a1e9a39b802cce551166e7861b1834c0f2936302ec91108dcfe9c66afa2555fd41cce8b3c57e66db92804590c4b6758a0acde49021cff5e7951e1d9c0c2f70e07807a5f059021f
6	K0	b44e3c56dff45afb56fff474dece853816f5c5577aa18996b73a1f970e01b09fa12d193fa98a70456f431360d6948e26a2ea94ff52b66ac71c03ab8ee5611b107d7a52366737184d97a1e9a39b802cce551166e7861b1834c0f2936302ec91108dcfe9c66afa2555fd41cce8b3c57e66db92804590c4b675

6.3.2 카운터 입력을 사용하고 IV = ∅인 경우

고정된 값	h (16진수)	0180
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	4db27290f3b1e3ef159394dd6a7f0c4362581354353ccbcdaa6f596ad74d64140c9a5116a0d3f54c1ec0fa9ed12142be
3	K(2)	90d667333626a71d26ecab83a70cd9bab3ec9d9e5656603ac1c55dac773d7d73cc2345dab8e28d688c193d0039a02eb9
4	K(n)	cca6f0a7f0fc5da5525733932783094dba37e05d1f1145eb96aaebb163ec33cb9d83546776e71739665b35e64d499ca6
5	result(n)	4db27290f3b1e3ef159394dd6a7f0c4362581354353ccbcdaa6f596ad74d64140c9a5116a0d3f54c1ec0fa9ed12142be90d667333626a71d26ecab83a70cd9bab3ec9d9e5656603ac1c55dac773d7d73cc2345dab8e28d688c193d0039a02eb9cca6f0a7f0fc5da5525733932783094dba37e05d1f1145eb96aaebb163ec33cb9d83546776e71739665b35e64d499ca6
6	K0	4db27290f3b1e3ef159394dd6a7f0c4362581354353ccbcdaa6f596ad74d64140c9a5116a0d3f54c1ec0fa9ed12142be90d667333626a71d26ecab83a70cd9bab3ec9d9e5656603ac1c55dac773d7d73cc2345dab8e28d688c193d0039a02eb9cca6f0a7f0fc5da5525733932783094dba37e05d1f1145eb

6.3.3 카운터 입력을 사용하지 않고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0180
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	5c87441ab93ba616417e0f30fe5ea77a0d6c8840fcbf5266d0fd4e2df6f8b8a7 df260fd4704c0c0d38d496b5292878c3
3	K(2)	a047a1dab325af1b916a09185971f084a62e9e34c1b023bff65aa05145f8d18b 891492a39ff3af123db530cf6e4e0da8
4	K(n)	da9eb8a4938364244c9e154c97031b26a4f2c212fae33546c1c2c0124bc2f2eb 6d5b054e30cff8e12916475771b0e549
5	result(n)	5c87441ab93ba616417e0f30fe5ea77a0d6c8840fcbf5266d0fd4e2df6f8b8a7 df260fd4704c0c0d38d496b5292878c3a047a1dab325af1b916a09185971f084 a62e9e34c1b023bff65aa05145f8d18b891492a39ff3af123db530cf6e4e0da8 da9eb8a4938364244c9e154c97031b26a4f2c212fae33546c1c2c0124bc2f2eb 6d5b054e30cff8e12916475771b0e549
6	K0	5c87441ab93ba616417e0f30fe5ea77a0d6c8840fcbf5266d0fd4e2df6f8b8a7 df260fd4704c0c0d38d496b5292878c3a047a1dab325af1b916a09185971f084 a62e9e34c1b023bff65aa05145f8d18b891492a39ff3af123db530cf6e4e0da8 da9eb8a4938364244c9e154c97031b26a4f2c212fae33546

6.3.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

고정된 값	h (16진수)	0180
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	972094736cad5812c1abca7784c0e45ae15600045982c2a8ec125934489240172e79f1ca82558c73a32a556a8a000172
3	K(2)	fe806a1762134349502a096d2d20b7bc75acdd51497a027cefb3bc33d6bfa8e0d1f3d67338c8eaf7f25653af59a49c03
4	K(n)	ba43bcbed5298507c7d9135c480fb873bb15d4d0bc1c76458aaaed88631098234b37af076d2851423632affb8de2fe51
5	result(n)	972094736cad5812c1abca7784c0e45ae15600045982c2a8ec125934489240172e79f1ca82558c73a32a556a8a000172fe806a1762134349502a096d2d20b7bc75acdd51497a027cefb3bc33d6bfa8e0d1f3d67338c8eaf7f25653af59a49c03ba43bcbed5298507c7d9135c480fb873bb15d4d0bc1c76458aaaed88631098234b37af076d2851423632affb8de2fe51
6	K0	972094736cad5812c1abca7784c0e45ae15600045982c2a8ec125934489240172e79f1ca82558c73a32a556a8a000172fe806a1762134349502a096d2d20b7bc75acdd51497a027cefb3bc33d6bfa8e0d1f3d67338c8eaf7f25653af59a49c03ba43bcbed5298507c7d9135c480fb873bb15d4d0bc1c7645

6.4 HMAC-LSH-512의 단계별 참조 구현값

6.4.1 카운터 입력을 사용하고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0200
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	7852cddfd3f9fd13a3d1d10fe1fcf4e9dd275a0d1cad7904cad1062704bed3a5 522aff8e3eeb5855a1d437fd9589c0a1a71201a6e3ba50ed0a3f3e5b81064dac
3	K(2)	e6b7e355e59202aedcce4009e2247e2f09f9ed88d3274e4144696c54514402fd 446585c205daa0c9e42d9eab427d2e190e7917101a709379f188c88e5bb86ae3
4	K(n)	7044e89c8b163fd327f23079fe88fc94452d1325aad14e8ab90901965d914061 19ddbc6474617c69f1ae9a874f89aa45c3886904164c32b3baa295acde241ad8
5	result(n)	7852cddfd3f9fd13a3d1d10fe1fcf4e9dd275a0d1cad7904cad1062704bed3a5 522aff8e3eeb5855a1d437fd9589c0a1a71201a6e3ba50ed0a3f3e5b81064dac e6b7e355e59202aedcce4009e2247e2f09f9ed88d3274e4144696c54514402fd 446585c205daa0c9e42d9eab427d2e190e7917101a709379f188c88e5bb86ae3 7044e89c8b163fd327f23079fe88fc94452d1325aad14e8ab90901965d914061 19ddbc6474617c69f1ae9a874f89aa45c3886904164c32b3baa295acde241ad8
6	K0	7852cddfd3f9fd13a3d1d10fe1fcf4e9dd275a0d1cad7904cad1062704bed3a5 522aff8e3eeb5855a1d437fd9589c0a1a71201a6e3ba50ed0a3f3e5b81064dac e6b7e355e59202aedcce4009e2247e2f09f9ed88d3274e4144696c54514402fd 446585c205daa0c9e42d9eab427d2e190e7917101a709379f188c88e5bb86ae3 7044e89c8b163fd327f23079fe88fc94452d1325aad14e8ab90901965d914061

6.4.2 카운터 입력을 사용하고 IV = ∅인 경우

고정된 값	h (16진수)	0200
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	7a0e5322cb5722d7260789d1db23f091ac567b002f8b38f3808f53394d73a783 48593b5583374185389ad89f61507061884e89bedeef5670fd868bb5d721a139
3	K(2)	50d1bd2fa87ca3287eea91d257432a6afdff3a394d42ee5a30d9966910e3c40c 58d1dd94d3ee8b010184de5ac795053043cfce920e990fedbecb107558497c46
4	K(n)	91b4fb2e86dd863d95483a5f2914feb12e20d58c8492eeb35ae1afc1c48def56 4d318827dca1687bc78a4e712b6eefb2ad452b6715ba9af75932e59699f2f7fd
5	result(n)	7a0e5322cb5722d7260789d1db23f091ac567b002f8b38f3808f53394d73a783 48593b5583374185389ad89f61507061884e89bedeef5670fd868bb5d721a139 50d1bd2fa87ca3287eea91d257432a6afdff3a394d42ee5a30d9966910e3c40c 58d1dd94d3ee8b010184de5ac795053043cfce920e990fedbecb107558497c46 91b4fb2e86dd863d95483a5f2914feb12e20d58c8492eeb35ae1afc1c48def56 4d318827dca1687bc78a4e712b6eefb2ad452b6715ba9af75932e59699f2f7fd
6	K0	7a0e5322cb5722d7260789d1db23f091ac567b002f8b38f3808f53394d73a783 48593b5583374185389ad89f61507061884e89bedeef5670fd868bb5d721a139 50d1bd2fa87ca3287eea91d257432a6afdff3a394d42ee5a30d9966910e3c40c 58d1dd94d3ee8b010184de5ac795053043cfce920e990fedbecb107558497c46 91b4fb2e86dd863d95483a5f2914feb12e20d58c8492eeb35ae1afc1c48def56

6.4.3 카운터 입력을 사용하지 않고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0200
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	1d8c871f96716391274870b059fec51548ef853210bf7ed9453fa0b0b6435809 56f603c003c120b074b9d52fc4badb6f7c1ee5c1bf9108c6a8f2a157183ecb5e
3	K(2)	7d9cdb12eea089a423741869c17f216edae2959435f942fe1f3ece39933f6f09 2241cdba237380dac4a12517b1539b55ae3165177bf1ce98d589a873be8926bf
4	K(n)	dc7501a1a86b463861db10fb878017b2c70b76cf71f55c0141e5861ca621d9b3 9973a3e05c4f2022535ede280dc020c1abb2573a282c3cf45ee5116d39a39ef3
5	result(n)	1d8c871f96716391274870b059fec51548ef853210bf7ed9453fa0b0b6435809 56f603c003c120b074b9d52fc4badb6f7c1ee5c1bf9108c6a8f2a157183ecb5e 7d9cdb12eea089a423741869c17f216edae2959435f942fe1f3ece39933f6f09 2241cdba237380dac4a12517b1539b55ae3165177bf1ce98d589a873be8926bf dc7501a1a86b463861db10fb878017b2c70b76cf71f55c0141e5861ca621d9b3 9973a3e05c4f2022535ede280dc020c1abb2573a282c3cf45ee5116d39a39ef3
6	K0	1d8c871f96716391274870b059fec51548ef853210bf7ed9453fa0b0b6435809 56f603c003c120b074b9d52fc4badb6f7c1ee5c1bf9108c6a8f2a157183ecb5e 7d9cdb12eea089a423741869c17f216edae2959435f942fe1f3ece39933f6f09 2241cdba237380dac4a12517b1539b55ae3165177bf1ce98d589a873be8926bf dc7501a1a86b463861db10fb878017b2c70b76cf71f55c0141e5861ca621d9b3

6.4.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

고정된 값	h (16진수)	0200
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	bca4f9601af22440b6cf32d3a39fc12e99cb1afa70097d664257f24bef4d1ba5 4c20345a301a64cae8894fcf11cdce85a4df9e3537a404744489f5c03f475fc1
3	K(2)	88437c2b4555372326edaa3756de7cf188970b6879ab820e7f45b0c7347dabae d0db553715d0d1efb7dfaef4c4df193d280a212fdd866b7859da205544aaeb6f
4	K(n)	93969a3f3030430c6029a516b761b213e17c5382d2c0083660ab230ea2fb21d2 2f2f7b674e4f95fd9a6186b56fcb259c9c8bf609edd9598e980554504869954e
5	result(n)	bca4f9601af22440b6cf32d3a39fc12e99cb1afa70097d664257f24bef4d1ba5 4c20345a301a64cae8894fcf11cdce85a4df9e3537a404744489f5c03f475fc1 88437c2b4555372326edaa3756de7cf188970b6879ab820e7f45b0c7347dabae d0db553715d0d1efb7dfaef4c4df193d280a212fdd866b7859da205544aaeb6f 93969a3f3030430c6029a516b761b213e17c5382d2c0083660ab230ea2fb21d2 2f2f7b674e4f95fd9a6186b56fcb259c9c8bf609edd9598e980554504869954e
6	K0	bca4f9601af22440b6cf32d3a39fc12e99cb1afa70097d664257f24bef4d1ba5 4c20345a301a64cae8894fcf11cdce85a4df9e3537a404744489f5c03f475fc1 88437c2b4555372326edaa3756de7cf188970b6879ab820e7f45b0c7347dabae d0db553715d0d1efb7dfaef4c4df193d280a212fdd866b7859da205544aaeb6f 93969a3f3030430c6029a516b761b213e17c5382d2c0083660ab230ea2fb21d2

6.5 HMAC-LSH-512-224의 단계별 참조 구현값

6.5.1 카운터 입력을 사용하고 IV ≠ ∅는 경우

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	d3143640c07a75dc1c21406bf5c8a5b33c68167878b2295367d3f909
3	K(2)	507945f5fe3eaab482651dd1248073d66259c5e75ab7b426196cbca8
4	K(n)	5f7a046281d0d8b5c963cd5bf5382787c6fe87e7826f93b633f532ee
5	result(n)	d3143640c07a75dc1c21406bf5c8a5b33c68167878b2295367d3f909507945f5 fe3eaab482651dd1248073d66259c5e75ab7b426196cbca85f7a046281d0d8b5 c963cd5bf5382787c6fe87e7826f93b633f532ee
6	K0	d3143640c07a75dc1c21406bf5c8a5b33c68167878b2295367d3f909507945f5 fe3eaab482651dd1248073d66259c5e75ab7b426196cbca85f7a046281d0d8b5 c963cd5bf538

6.5.2 카운터 입력을 사용하고 IV = ∅인 경우

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	f30a6558d356497683dba43b72619a68486ce67a316acca03132b58b
3	K(2)	67bc5c70ee079c12c63d629e290a230097a7b4f945fba1a1828dc3c2
4	K(n)	ddb60df3521c1e7aef422a502fab9a7eb0b1fc18624926c5f6e3b931
5	result(n)	f30a6558d356497683dba43b72619a68486ce67a316acca03132b58b67bc5c70ee079c12c63d629e290a230097a7b4f945fba1a1828dc3c2ddb60df3521c1e7aef422a502fab9a7eb0b1fc18624926c5f6e3b931
6	K0	f30a6558d356497683dba43b72619a68486ce67a316acca03132b58b67bc5c70ee079c12c63d629e290a230097a7b4f945fba1a1828dc3c2ddb60df3521c1e7aef422a502fab

6.5.3 카운터 입력을 사용하지 않고 IV ≠ ∅는 경우

고정된 값	h (16진수)	00e0
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	1cb95385cd24547956e77c99a1d61791e20f029805d98d17ff81f7d6
3	K(2)	7b32c6845c00a770e5c1367544e909907326360d1a37cd05f42ba2b6
4	K(n)	00e851edb8b112c905977d8d0552343538a8ca25ad28b3651846f351
5	result(n)	1cb95385cd24547956e77c99a1d61791e20f029805d98d17ff81f7d67b32c6845c00a770e5c1367544e909907326360d1a37cd05f42ba2b600e851edb8b112c905977d8d0552343538a8ca25ad28b3651846f351
6	K0	1cb95385cd24547956e77c99a1d61791e20f029805d98d17ff81f7d67b32c6845c00a770e5c1367544e909907326360d1a37cd05f42ba2b600e851edb8b112c905977d8d0552

6.5.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

고정된 값	h (16진수)	00e0
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	4ba2946bfad7fb7c97253bf58485b8e90db1c5d56e2c673647dc0af1
3	K(2)	156c24a3cde9885ce1ace475749deb7e611d54acabc1a81c60b8f75b
4	K(n)	40d672a9510b86959f897833f103e750a7dfe956fb096225a2986d3b
5	result(n)	4ba2946bfad7fb7c97253bf58485b8e90db1c5d56e2c673647dc0af1156c24a3 cde9885ce1ace475749deb7e611d54acabc1a81c60b8f75b40d672a9510b8695 9f897833f103e750a7dfe956fb096225a2986d3b
6	K0	4ba2946bfad7fb7c97253bf58485b8e90db1c5d56e2c673647dc0af1156c24a3 cde9885ce1ace475749deb7e611d54acabc1a81c60b8f75b40d672a9510b8695 9f897833f103

6.6 HMAC-LSH-512-256의 단계별 참조 구현값

6.6.1 카운터 입력을 사용하고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	bc0b11b74f4d14df159d4a411adca918315219d1313c511dd3e69d633a601611
3	K(2)	293cc3a795940d9232037fb0dccf98b7bf8f27a563d5258756ac8d1e52091ee4
4	K(n)	4d175e9dfb6924c83ddc6674edfc6b436988f655f5053745d4ffe02eec25ae50
5	result(n)	bc0b11b74f4d14df159d4a411adca918315219d1313c511dd3e69d633a601611 293cc3a795940d9232037fb0dccf98b7bf8f27a563d5258756ac8d1e52091ee4 4d175e9dfb6924c83ddc6674edfc6b436988f655f5053745d4ffe02eec25ae50
6	K0	bc0b11b74f4d14df159d4a411adca918315219d1313c511dd3e69d633a601611 293cc3a795940d9232037fb0dccf98b7bf8f27a563d5258756ac8d1e52091ee4 4d175e9dfb6924c83ddc6674edfc6b43

6.6.2 카운터 입력을 사용하고 IV = ∅인 경우

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	c6e40f6d7784f8940d108d72f8845d169c1d15c88ca393b901d2afa72fcee813
3	K(2)	93e9fadc2902f44cdc5fb6940ded1cc9f3e9a07f32a4185edc05941fefd31626
4	K(n)	71e72458b0f0c74ef59559f7ae934cb34c6bae5fcc6d34390d68b7eed0b58530
5	result(n)	c6e40f6d7784f8940d108d72f8845d169c1d15c88ca393b901d2afa72fcee813 93e9fadc2902f44cdc5fb6940ded1cc9f3e9a07f32a4185edc05941fefd31626 71e72458b0f0c74ef59559f7ae934cb34c6bae5fcc6d34390d68b7eed0b58530
6	K0	c6e40f6d7784f8940d108d72f8845d169c1d15c88ca393b901d2afa72fcee813 93e9fadc2902f44cdc5fb6940ded1cc9f3e9a07f32a4185edc05941fefd31626 71e72458b0f0c74ef59559f7ae934cb3

6.6.3 카운터 입력을 사용하지 않고 IV ≠ ∅는 경우

고정된 값	h (16진수)	0100
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	a5bbde22c561a924b56a2b810c78cbbf8cd8f9d2c30120ba502c19c3e0ee8e21
3	K(2)	3b4e74fbda6c3db5ccdfd6feafea88dc107705e1904223a2a0a35f5dbfe65173
4	K(n)	4112c64f916c45aa3d698d2b0c8cffe6b44c2690dbf12dfc458967fa19755842
5	result(n)	a5bbde22c561a924b56a2b810c78cbbf8cd8f9d2c30120ba502c19c3e0ee8e21 3b4e74fbda6c3db5ccdfd6feafea88dc107705e1904223a2a0a35f5dbfe65173 4112c64f916c45aa3d698d2b0c8cffe6b44c2690dbf12dfc458967fa19755842
6	K0	a5bbde22c561a924b56a2b810c78cbbf8cd8f9d2c30120ba502c19c3e0ee8e21 3b4e74fbda6c3db5ccdfd6feafea88dc107705e1904223a2a0a35f5dbfe65173 4112c64f916c45aa3d698d2b0c8cffe6

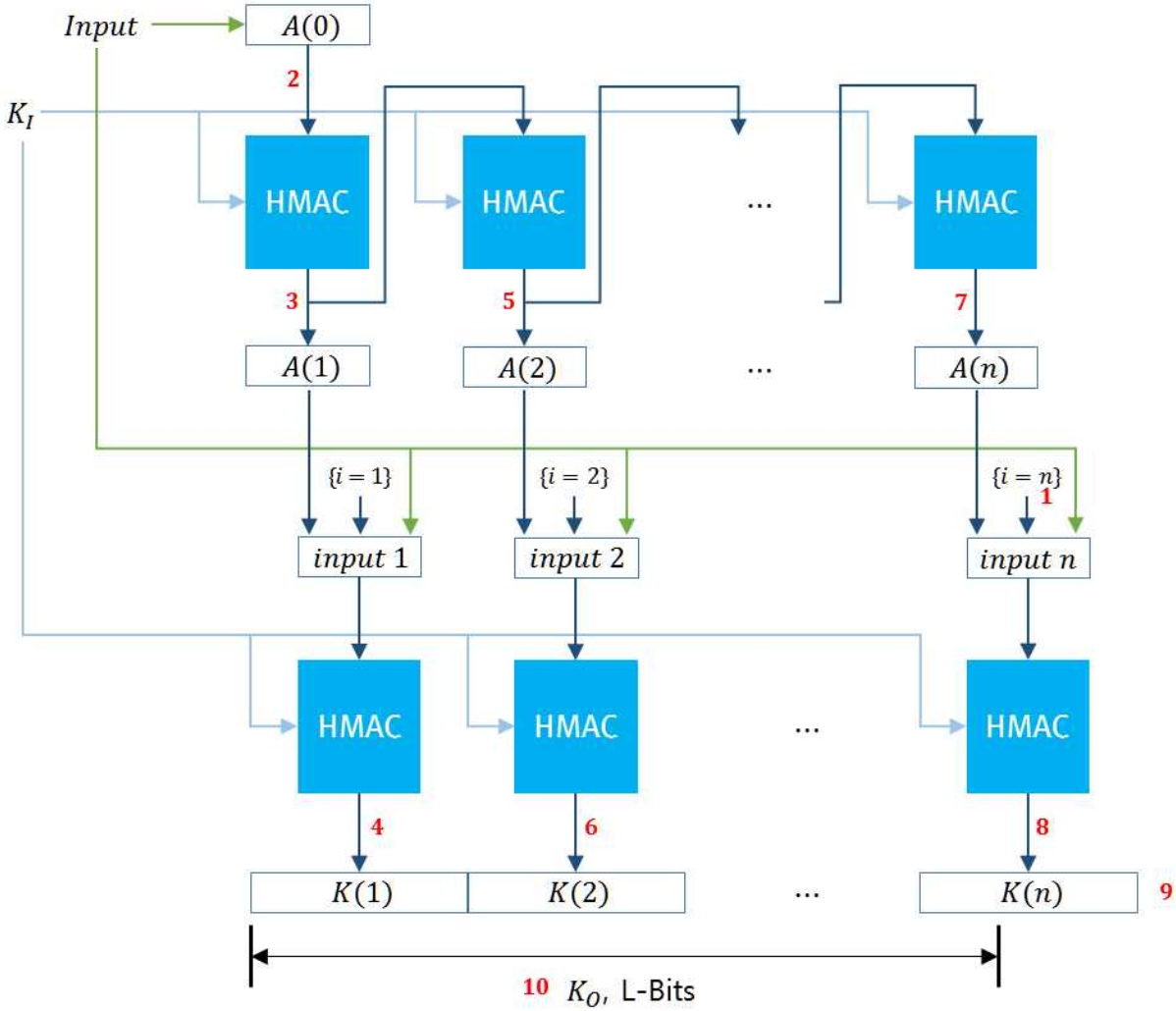
6.6.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

고정된 값	h (16진수)	0100
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	IV (16진수)	-
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	519b0a60378cfe8737f42db20cccb0c2fc61ff0c035f42446c0be43229884528
3	K(2)	45b9ec80d234dbc7d0fd677cb11384cff2b9899e7496bfa49d30d2a9e65de951
4	K(n)	445de708b05930f0d5fa48c1e9bfca2acc8730f9d998c9f1feab8f0f103cb624
5	result(n)	519b0a60378cfe8737f42db20cccb0c2fc61ff0c035f42446c0be43229884528 45b9ec80d234dbc7d0fd677cb11384cff2b9899e7496bfa49d30d2a9e65de951 445de708b05930f0d5fa48c1e9bfca2acc8730f9d998c9f1feab8f0f103cb624
6	K0	519b0a60378cfe8737f42db20cccb0c2fc61ff0c035f42446c0be43229884528 45b9ec80d234dbc7d0fd677cb11384cff2b9899e7496bfa49d30d2a9e65de951 445de708b05930f0d5fa48c1e9bfca2a

7 더블-파이프라인 반복 모드를 이용한 키 유도 함수 참조 구현값

※ $Input = Label \,||\, 0x00 \,||\, Context \,||\, [L]_2$



7.1 HMAC-LSH-224의 단계별 참조 구현값

7.1.1 카운터 입력을 사용한 경우

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0230
3	A(1)	7c08b0cb988cad74ada55df498f4443c1f2b178be01163a86d97a6e2
4	K(1)	12707f5c7d75514db578db9864386238ddbd39a7ee57490004bcda5e
5	A(2)	6c4cf92cadbae765889ef11912ab21b7df7324ddd6e2ecd30f396c19
6	K(2)	a4f892869c516d2034134c3b5f74f2c780827745e5786cf79d38dcdb
7	A(n)	627bd19f6379a32bb8437a8ca2e912b31d2ef109fb2ea8c03852594c
8	K(n)	8ac172c3b473936cacb10dfd25fa904850ada7b7a3df2b6f6fea52f3
9	result(n)	12707f5c7d75514db578db9864386238ddbd39a7ee57490004bcda5ea4f89286 9c516d2034134c3b5f74f2c780827745e5786cf79d38dcdb8ac172c3b473936c acb10dfd25fa904850ada7b7a3df2b6f6fea52f3
10	K0	12707f5c7d75514db578db9864386238ddbd39a7ee57490004bcda5ea4f89286 9c516d2034134c3b5f74f2c780827745e5786cf79d38dcdb8ac172c3b473936c acb10dfd25fa

7.1.2 카운터 입력을 사용하지 않는 경우

고정된 값	h (16진수)	00e0
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0230
3	A(1)	7c08b0cb988cad74ada55df498f4443c1f2b178be01163a86d97a6e2
4	K(1)	efb1815b843a887018467f0096c91d51949e86942610d82ad0d8ed27
5	A(2)	6c4cf92cadbae765889ef11912ab21b7df7324ddd6e2ecd30f396c19
6	K(2)	097831084f14a6ff6bbd69494c0c5ceb39fc90888a4ed8bd597fd1c6
7	A(n)	627bd19f6379a32bb8437a8ca2e912b31d2ef109fb2ea8c03852594c
8	K(n)	fb51a14a063547ef8729faf41e27a7f4e2789d91dd27f8d16364ce6a
9	result(n)	efb1815b843a887018467f0096c91d51949e86942610d82ad0d8ed2709783108 4f14a6ff6bbd69494c0c5ceb39fc90888a4ed8bd597fd1c6fb51a14a063547ef 8729faf41e27a7f4e2789d91dd27f8d16364ce6a
10	K0	efb1815b843a887018467f0096c91d51949e86942610d82ad0d8ed2709783108 4f14a6ff6bbd69494c0c5ceb39fc90888a4ed8bd597fd1c6fb51a14a063547ef 8729faf41e27

7.2 HMAC-LSH-256의 단계별 참조 구현값

7.2.1 카운터 입력을 사용한 경우

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0280
3	A(1)	5ebb4e14afaa8db0402221f9165ff6f2ed7d20c25a679b84d1013ba5695fea24
4	K(1)	fbac25ed4ab808be052a86694e3ebcc6726615fa066b7e2d569afc2f2db7f4b1
5	A(2)	87b59f8a111ac71bef0e7bd319ffe2333dce64e8f3fde70378173d97f6152962
6	K(2)	22f76746cb91453544d479468778c8b01fcbb399f326bc2715e23c56e9a40349
7	A(n)	b66bc22f9c77c39c1f2d2b79a31143732bda8300f373f52f6b1ee4a602e81d6e
8	K(n)	1231ea3f529c06a33d809d961e2cd2bda0e02c3371199a234fb5b068a114726c
9	result(n)	fbac25ed4ab808be052a86694e3ebcc6726615fa066b7e2d569afc2f2db7f4b1 22f76746cb91453544d479468778c8b01fcbb399f326bc2715e23c56e9a40349 1231ea3f529c06a33d809d961e2cd2bda0e02c3371199a234fb5b068a114726c
10	K0	fbac25ed4ab808be052a86694e3ebcc6726615fa066b7e2d569afc2f2db7f4b1 22f76746cb91453544d479468778c8b01fcbb399f326bc2715e23c56e9a40349 1231ea3f529c06a33d809d961e2cd2bd

7.2.2 카운터 입력을 사용하지 않는 경우

고정된 값	h (16진수)	0100
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0280
3	A(1)	5ebb4e14afaa8db0402221f9165ff6f2ed7d20c25a679b84d1013ba5695fea24
4	K(1)	1fc82ad177800890ec778860b02c362c49751292bf32dc739b77bc8bc76cf5a3
5	A(2)	87b59f8a111ac71bef0e7bd319ffe2333dce64e8f3fde70378173d97f6152962
6	K(2)	a1a49554e6ddf4b64f071a72356717ffacf4097f1e90ad734aab71f07e479244
7	A(n)	b66bc22f9c77c39c1f2d2b79a31143732bda8300f373f52f6b1ee4a602e81d6e
8	K(n)	9e0c4910aaa7c160e25c6af914bddafdcf92c898fcd259eef892f87ff8ef3d17
9	result(n)	1fc82ad177800890ec778860b02c362c49751292bf32dc739b77bc8bc76cf5a3 a1a49554e6ddf4b64f071a72356717ffacf4097f1e90ad734aab71f07e479244 9e0c4910aaa7c160e25c6af914bddafdcf92c898fcd259eef892f87ff8ef3d17
10	K0	1fc82ad177800890ec778860b02c362c49751292bf32dc739b77bc8bc76cf5a3 a1a49554e6ddf4b64f071a72356717ffacf4097f1e90ad734aab71f07e479244 9e0c4910aaa7c160e25c6af914bddafd

7.3 HMAC-LSH-384의 단계별 참조 구현값

7.3.1 카운터 입력을 사용한 경우

고정된 값	h (16진수)	0180
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabb0000112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899aabb03c0
3	A(1)	972094736cad5812c1abca7784c0e45ae15600045982c2a8ec125934489240172e79f1ca82558c73a32a556a8a000172
4	K(1)	54e1b3262c5db75532b31ddd6ccb6a1c0e1e661c88efc3be6ca5e9d436ee1e36b333c566f239b16536219ab792ac1ec7
5	A(2)	fa4cbf56a0d8b9061104118187b8968eb0c1d3172c3faba9abc0999a8497ad01a664714a87c82409214cc3b5421b8e7d
6	K(2)	aa3f7c541d94d1da8704ecc432a269df9b3d594168b13e576b41b15b4bc5f0fe73dbfd9a391bda6ae7397263578f89f8
7	A(n)	f594c92088b0ab051bb5760c2ddf6b438c5e8ff4e0a1a8738e448f58aac75036c412d260ce352cc709ad16c91989b996
8	K(n)	8b840224c317909129dd2d0e6d6042beb12bf35dca7f1c359735102165d37e41541d79fb7e638ecc89fe22621910003f
9	result(n)	54e1b3262c5db75532b31ddd6ccb6a1c0e1e661c88efc3be6ca5e9d436ee1e36b333c566f239b16536219ab792ac1ec7aa3f7c541d94d1da8704ecc432a269df9b3d594168b13e576b41b15b4bc5f0fe73dbfd9a391bda6ae7397263578f89f88b840224c317909129dd2d0e6d6042beb12bf35dca7f1c359735102165d37e41541d79fb7e638ecc89fe22621910003f
10	K0	54e1b3262c5db75532b31ddd6ccb6a1c0e1e661c88efc3be6ca5e9d436ee1e36b333c566f239b16536219ab792ac1ec7aa3f7c541d94d1da8704ecc432a269df9b3d594168b13e576b41b15b4bc5f0fe73dbfd9a391bda6ae7397263578f89f88b840224c317909129dd2d0e6d6042beb12bf35dca7f1c35

7.3.2 카운터 입력을 사용하지 않는 경우

고정된 값	h (16진수)	0180
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb03c0
3	A(1)	972094736cad5812c1abca7784c0e45ae15600045982c2a8ec12593448924017 2e79f1ca82558c73a32a556a8a000172
4	K(1)	fe806a1762134349502a096d2d20b7bc75acdd51497a027cefb3bc33d6bfa8e0 d1f3d67338c8eaf7f25653af59a49c03
5	A(2)	fa4cbf56a0d8b9061104118187b8968eb0c1d3172c3faba9abc0999a8497ad01 a664714a87c82409214cc3b5421b8e7d
6	K(2)	9f6d78e04012d0737c641142db4f2bc2d792e860e716f5cce2f5f3ff1c37aea5 9d1f2b4865a43e4375cd83e3941af5ee
7	A(n)	f594c92088b0ab051bb5760c2ddf6b438c5e8ff4e0a1a8738e448f58aac75036 c412d260ce352cc709ad16c91989b996
8	K(n)	6ac4df9b2e2c7bc2a8049bcfaa7920ccf83ae92e168ebbe33ffd7a9f11835f43 f05a3fe0aa8e7593c1d167fbab1177e8
9	result(n)	fe806a1762134349502a096d2d20b7bc75acdd51497a027cefb3bc33d6bfa8e0 d1f3d67338c8eaf7f25653af59a49c039f6d78e04012d0737c641142db4f2bc2 d792e860e716f5cce2f5f3ff1c37aea59d1f2b4865a43e4375cd83e3941af5ee 6ac4df9b2e2c7bc2a8049bcfaa7920ccf83ae92e168ebbe33ffd7a9f11835f43 f05a3fe0aa8e7593c1d167fbab1177e8
10	K0	fe806a1762134349502a096d2d20b7bc75acdd51497a027cefb3bc33d6bfa8e0 d1f3d67338c8eaf7f25653af59a49c039f6d78e04012d0737c641142db4f2bc2 d792e860e716f5cce2f5f3ff1c37aea59d1f2b4865a43e4375cd83e3941af5ee 6ac4df9b2e2c7bc2a8049bcfaa7920ccf83ae92e168ebbe3

7.4 HMAC-LSH-512의 단계별 참조 구현값

7.4.1 카운터 입력을 사용한 경우

고정된 값	h (16진수)	0200
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0500
3	A(1)	bca4f9601af22440b6cf32d3a39fc12e99cb1afa70097d664257f24bef4d1ba5 4c20345a301a64cae8894fcf11cdce85a4df9e3537a404744489f5c03f475fc1
4	K(1)	a7fb18da6ae22b62060ba405e3dd0460b9270218430d13f04df2e96c84405dfd 99ff534cef71e7a4a8070d6a680aaf4150e9f36c38fe1fec0d9e5522632aed3d
5	A(2)	1d565e5068d4536af86e723b22096650b455a29a324b59cf4cf85e6484e83f73 1c8787350e29a35ef64bfe0666ad13ab06cb20b480d372e621800e60e4dc7d5b
6	K(2)	da63877086448c2d4fd61ee9fbd9126fb90eb058fc90d17e81cf16bab5f8e8d3 c6cea2d6e2df93f6cecb957b8e170918a42283724a263965c3e0190ae6c9000f
7	A(n)	77c1b9ad2e35643ffc4b6b8676bc37586af2909aa3126fe19a5459bd6b743ec2 631603f01fc856ae89e9b4699a898c0df942678febeb55364b16e17012ffb671
8	K(n)	81f851201524c00667a79a50c52681a6123080b65eec75b5f0934ce8b19441b8 be6aacc5847e4ab02e7bd0334e181c373033ddfdac5e831484f7daaaba8b925b
9	result(n)	a7fb18da6ae22b62060ba405e3dd0460b9270218430d13f04df2e96c84405dfd 99ff534cef71e7a4a8070d6a680aaf4150e9f36c38fe1fec0d9e5522632aed3d da63877086448c2d4fd61ee9fbd9126fb90eb058fc90d17e81cf16bab5f8e8d3 c6cea2d6e2df93f6cecb957b8e170918a42283724a263965c3e0190ae6c9000f 81f851201524c00667a79a50c52681a6123080b65eec75b5f0934ce8b19441b8 be6aacc5847e4ab02e7bd0334e181c373033ddfdac5e831484f7daaaba8b925b
10	K0	a7fb18da6ae22b62060ba405e3dd0460b9270218430d13f04df2e96c84405dfd 99ff534cef71e7a4a8070d6a680aaf4150e9f36c38fe1fec0d9e5522632aed3d da63877086448c2d4fd61ee9fbd9126fb90eb058fc90d17e81cf16bab5f8e8d3 c6cea2d6e2df93f6cecb957b8e170918a42283724a263965c3e0190ae6c9000f 81f851201524c00667a79a50c52681a6123080b65eec75b5f0934ce8b19441b8

7.4.2 카운터 입력을 사용하지 않는 경우

고정된 값	h (16진수)	0200
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0500
3	A(1)	bca4f9601af22440b6cf32d3a39fc12e99cb1afa70097d664257f24bef4d1ba5 4c20345a301a64cae8894fcf11cdce85a4df9e3537a404744489f5c03f475fc1
4	K(1)	88437c2b4555372326edaa3756de7cf188970b6879ab820e7f45b0c7347dabae d0db553715d0d1efb7dfaef4c4df193d280a212fdd866b7859da205544aaeb6f
5	A(2)	1d565e5068d4536af86e723b22096650b455a29a324b59cf4cf85e6484e83f73 1c8787350e29a35ef64bfe0666ad13ab06cb20b480d372e621800e60e4dc7d5b
6	K(2)	8d854d0106943ef2f7865839b30a77ca5eea59603e5bf4a22f1e9e0e76d96597 a0188d4b9f1e9a72f3902572a0783a798c2465d265be0df13c5b50192e6e0c7e
7	A(n)	77c1b9ad2e35643ffc4b6b8676bc37586af2909aa3126fe19a5459bd6b743ec2 631603f01fc856ae89e9b4699a898c0df942678febeb55364b16e17012ffb671
8	K(n)	d2957900a7731102fa6021ea7f26aa16f60b1aa12215b084fedd98e81db515e4 72dccf7c4accaf616b27ed12d2a9473173c6cc948e434151b3b76424dafb97e6
9	result(n)	88437c2b4555372326edaa3756de7cf188970b6879ab820e7f45b0c7347dabae d0db553715d0d1efb7dfaef4c4df193d280a212fdd866b7859da205544aaeb6f 8d854d0106943ef2f7865839b30a77ca5eea59603e5bf4a22f1e9e0e76d96597 a0188d4b9f1e9a72f3902572a0783a798c2465d265be0df13c5b50192e6e0c7e d2957900a7731102fa6021ea7f26aa16f60b1aa12215b084fedd98e81db515e4 72dccf7c4accaf616b27ed12d2a9473173c6cc948e434151b3b76424dafb97e6
10	K0	88437c2b4555372326edaa3756de7cf188970b6879ab820e7f45b0c7347dabae d0db553715d0d1efb7dfaef4c4df193d280a212fdd866b7859da205544aaeb6f 8d854d0106943ef2f7865839b30a77ca5eea59603e5bf4a22f1e9e0e76d96597 a0188d4b9f1e9a72f3902572a0783a798c2465d265be0df13c5b50192e6e0c7e d2957900a7731102fa6021ea7f26aa16f60b1aa12215b084fedd98e81db515e4

7.5 HMAC-LSH-512-224의 단계별 참조 구현값

7.5.1 카운터 입력을 사용한 경우

고정된 값	h (16진수)	00e0
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0230
3	A(1)	4ba2946bfad7fb7c97253bf58485b8e90db1c5d56e2c673647dc0af1
4	K(1)	303ee9980ebae713cc93c7b7b4ad008eb75ef032b7f12cf405822207
5	A(2)	c60e1d58bf5b0c544f6908b6aece6b1cf37d19797b6dd0b01fa7dd7b
6	K(2)	901a7ec14ae82fa67ae7f555064267fdc6723171b745c97f69f3c514
7	A(n)	076ca5b779536cdbe54d6cfb64379cdfbc038c02b3dc4f804e2ebbbe
8	K(n)	8e7a0996e1ab4044484bd2f3c507ea80ed4c71165913622aac01b5fb
9	result(n)	303ee9980ebae713cc93c7b7b4ad008eb75ef032b7f12cf405822207901a7ec1 4ae82fa67ae7f555064267fdc6723171b745c97f69f3c5148e7a0996e1ab4044 484bd2f3c507ea80ed4c71165913622aac01b5fb
10	K0	303ee9980ebae713cc93c7b7b4ad008eb75ef032b7f12cf405822207901a7ec1 4ae82fa67ae7f555064267fdc6723171b745c97f69f3c5148e7a0996e1ab4044 484bd2f3c507

7.5.2 카운터 입력을 사용하지 않는 경우

고정된 값	h (16진수)	00e0
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabb
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0230
3	A(1)	4ba2946bfad7fb7c97253bf58485b8e90db1c5d56e2c673647dc0af1
4	K(1)	156c24a3cde9885ce1ace475749deb7e611d54acabc1a81c60b8f75b
5	A(2)	c60e1d58bf5b0c544f6908b6aece6b1cf37d19797b6dd0b01fa7dd7b
6	K(2)	2d2d02204e522eab39e8be3ef84fbd435bbe14481a266aa1b26f1425
7	A(n)	076ca5b779536cdbe54d6cfb64379cdfbc038c02b3dc4f804e2ebbbe
8	K(n)	1f0b4df95e82c6f96c27cf0f1d8ae32acd9ca3d717919babf5d2bc45
9	result(n)	156c24a3cde9885ce1ace475749deb7e611d54acabc1a81c60b8f75b2d2d0220 4e522eab39e8be3ef84fbd435bbe14481a266aa1b26f14251f0b4df95e82c6f9 6c27cf0f1d8ae32acd9ca3d717919babf5d2bc45
10	K0	156c24a3cde9885ce1ace475749deb7e611d54acabc1a81c60b8f75b2d2d0220 4e522eab39e8be3ef84fbd435bbe14481a266aa1b26f14251f0b4df95e82c6f9 6c27cf0f1d8a

7.6 HMAC-LSH-512-256의 단계별 참조 구현값

7.6.1 카운터 입력을 사용한 경우

고정된 값	h (16진수)	0100
	r (10진수)	8
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0280
3	A(1)	519b0a60378cfe8737f42db20cccb0c2fc61ff0c035f42446c0be43229884528
4	K(1)	a0f72db1e3b4251e78dba3f9f2465429037e507bbd06337778f533dc9bd83776
5	A(2)	bf1ec2145766fa6b55fe810d676586da5d34e5e087bd019b74d9d6dd619a336b
6	K(2)	1b073f98bdcad0c1ec4147187cbfcf2b82fbe28099741cb8b7c4502f66b78686
7	A(n)	8da04e9791c4165428af2e70a130ba44266b7953365e29df8c21b6e9d99cd9ba
8	K(n)	b7133caf6fca9ef2b9858b9f2214cafe902580d2b355fa67ab64e74fed14a6ef
9	result(n)	a0f72db1e3b4251e78dba3f9f2465429037e507bbd06337778f533dc9bd83776 1b073f98bdcad0c1ec4147187cbfcf2b82fbe28099741cb8b7c4502f66b78686 b7133caf6fca9ef2b9858b9f2214cafe902580d2b355fa67ab64e74fed14a6ef
10	K0	a0f72db1e3b4251e78dba3f9f2465429037e507bbd06337778f533dc9bd83776 1b073f98bdcad0c1ec4147187cbfcf2b82fbe28099741cb8b7c4502f66b78686 b7133caf6fca9ef2b9858b9f2214cafe

7.6.2 카운터 입력을 사용하지 않는 경우

고정된 값	h (16진수)	0100
	r (10진수)	0
입력	KI (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	Label (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	Context (16진수)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb0280
3	A(1)	519b0a60378cfe8737f42db20cccb0c2fc61ff0c035f42446c0be43229884528
4	K(1)	45b9ec80d234dbc7d0fd677cb11384cff2b9899e7496bfa49d30d2a9e65de951
5	A(2)	bf1ec2145766fa6b55fe810d676586da5d34e5e087bd019b74d9d6dd619a336b
6	K(2)	944dbceb1e2244f0b98dfb672a38eef749135378cefa23c1028832dd25e18598
7	A(n)	8da04e9791c4165428af2e70a130ba44266b7953365e29df8c21b6e9d99cd9ba
8	K(n)	2811b03acd0b7cfe7155ea60e76c5e5b5d587d89cd2464e1fe54585b61c31474
9	result(n)	45b9ec80d234dbc7d0fd677cb11384cff2b9899e7496bfa49d30d2a9e65de951 944dbceb1e2244f0b98dfb672a38eef749135378cefa23c1028832dd25e18598 2811b03acd0b7cfe7155ea60e76c5e5b5d587d89cd2464e1fe54585b61c31474
10	K0	45b9ec80d234dbc7d0fd677cb11384cff2b9899e7496bfa49d30d2a9e65de951 944dbceb1e2244f0b98dfb672a38eef749135378cefa23c1028832dd25e18598 2811b03acd0b7cfe7155ea60e76c5e5b

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 800-108, “Recommendation for Key Derivation Using Pseudorandom Functions”, 2009. 8.

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

※ 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)