TTA Standard

정보통신단체표준(국문표준)

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

HMAC 기반 키 유도 함수
- 제2부: 해시 함수 SHA-2

HMAC-based Key Derivation Functions
- 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 HMAC 기반 키 유도 함수에 해시 함수 SHA-2를 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 키 유도 함수의 기반 해시 함수로 ISO/IEC 10118-3에 규정된 해시 함수 SHA-2를 적용한 결과로, 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 HMAC based on SHA-2 about implementation conformance.

2 Summary

The standard specifies the test vectors of KDF used as HMAC(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 KDF based on HMAC mechanism specified in Part 1: General.
And, KDF and SHA-2 conform to the specifications of each standard.

목 차

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

1 적용 범위

이 표준은 제1부 일반에서 정의한 HMAC 기반 키 유도 함수를 해시 함수 SHA-2로 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	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> 의사난수함수

구분	알고리즘	
의사 난수 함수 (PRF)	HMAC-SHA-2	HMAC-SHA-224
		HMAC-SHA-256
		HMAC-SHA-384
		HMAC-SHA-512

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-SHA-224
	5.2	HMAC-SHA-256
	5.3	HMAC-SHA-384
	5.4	HMAC-SHA-512
(6절) 피드백 모드를 이용한 키 유도 함수 참조 구현값	6.1	HMAC-SHA-224
	6.2	HMAC-SHA-256
	6.3	HMAC-SHA-384
	6.4	HMAC-SHA-512
(7절) 더블-파이프라인 반복 모드를 이용한 키 유도 함수 참조 구현값	7.1	HMAC-SHA-224
	7.2	HMAC-SHA-256
	7.3	HMAC-SHA-384
	7.4	HMAC-SHA-512

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

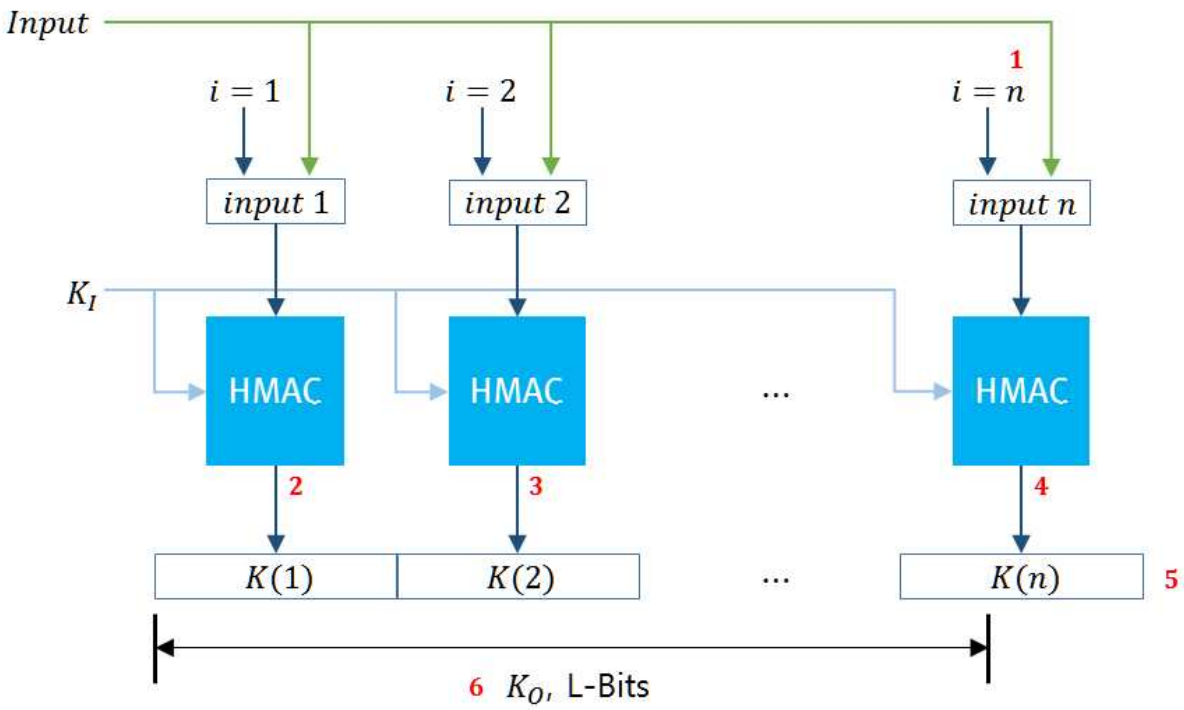
- 해당없음

4 약어

- 해당없음

5 카운터 모드를 이용한 키 유도 함수 참조 구현값

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



5.1 HMAC-SHA-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)	e50dccef026d0d446f34c90f919bbff924cb57e09caa9ec30f05eaba
3	K(2)	00619c4998eb35f28295dac8ef49efd6865c7e5f847d62daee89339d
4	K(n)	fc04d77a29a3edf406ffe053219dd6105a774336a2dc51d571f69eaf
5	result(n)	e50dccef026d0d446f34c90f919bbff924cb57e09caa9ec30f05eaba00619c4998eb35f28295dac8ef49efd6865c7e5f847d62daee89339dfc04d77a29a3edf406ffe053219dd6105a774336a2dc51d571f69eaf
6	K0	e50dccef026d0d446f34c90f919bbff924cb57e09caa9ec30f05eaba00619c4998eb35f28295dac8ef49efd6865c7e5f847d62daee89339dfc04d77a29a3edf406ffe053219d

5.2 HMAC-SHA-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)	8da6974e8e8683042d73b24239658e7e2cef712e9335059cd34d5b2f8a25e9c9
3	K(2)	4a6e8b64bddc77688aad7390ce08e9107bf1d165edf0c41dad8e9195549da3b2
4	K(n)	ef33b2af0c803c6d36c392f745753ab94ad1856241d304ad987ee043f0eba010
5	result(n)	8da6974e8e8683042d73b24239658e7e2cef712e9335059cd34d5b2f8a25e9c9 4a6e8b64bddc77688aad7390ce08e9107bf1d165edf0c41dad8e9195549da3b2 ef33b2af0c803c6d36c392f745753ab94ad1856241d304ad987ee043f0eba010
6	K0	8da6974e8e8683042d73b24239658e7e2cef712e9335059cd34d5b2f8a25e9c9 4a6e8b64bddc77688aad7390ce08e9107bf1d165edf0c41dad8e9195549da3b2 ef33b2af0c803c6d36c392f745753ab9

5.3 HMAC-SHA-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

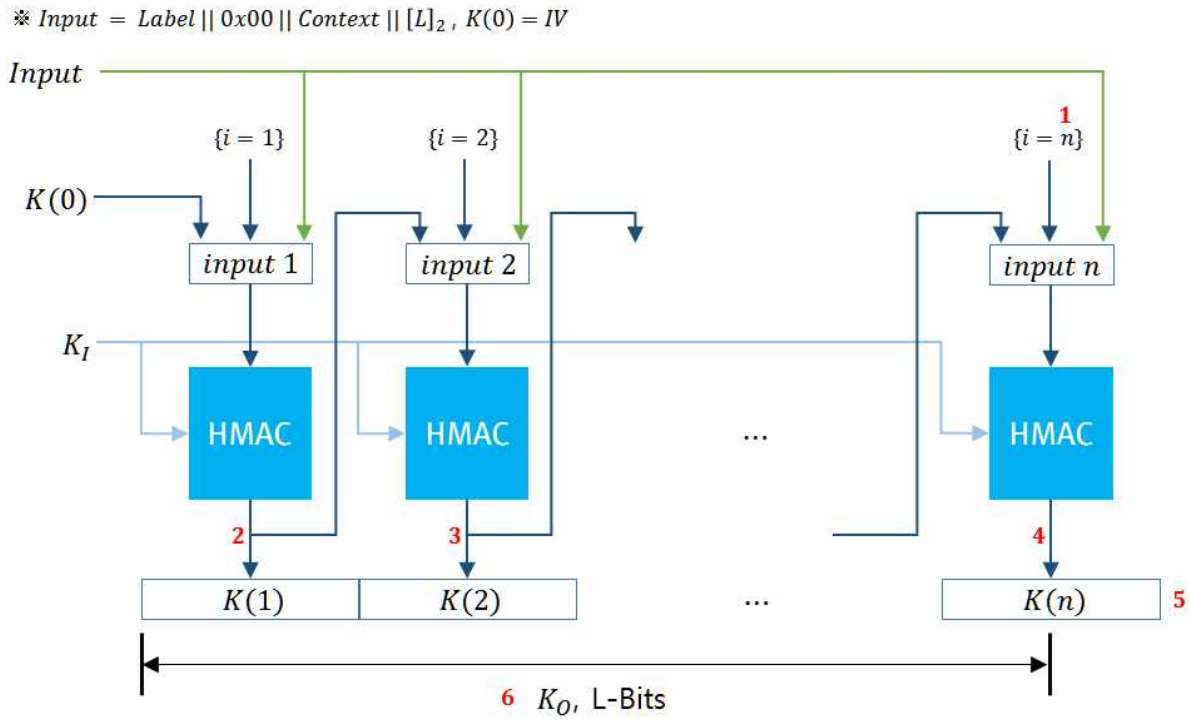
위치	변수	중간값(16진수)
1	n	3
2	K(1)	aa66fcf02050a4a0ae12eb9a7be4263374fcd08127634e05d6afe4237d10a6e75042ab595d9b08d72bcbd11d5cf727e9
3	K(2)	420f220a19aad1e5aaf156aebf70e6dfdd0d9f350548cbc175e29c533138f99272ad7767952258d0d30b2d749d41cafd
4	K(n)	0234aaa094dd2189c49f6568b4c001dd52d8ad6b63c724f822e64e9a298fe7c049c469889967154198d75751b93dd03d
5	result(n)	aa66fcf02050a4a0ae12eb9a7be4263374fcd08127634e05d6afe4237d10a6e75042ab595d9b08d72bcbd11d5cf727e9420f220a19aad1e5aaf156aebf70e6dfdd0d9f350548cbc175e29c533138f99272ad7767952258d0d30b2d749d41cafd0234aaa094dd2189c49f6568b4c001dd52d8ad6b63c724f822e64e9a298fe7c049c469889967154198d75751b93dd03d
6	K0	aa66fcf02050a4a0ae12eb9a7be4263374fcd08127634e05d6afe4237d10a6e75042ab595d9b08d72bcbd11d5cf727e9420f220a19aad1e5aaf156aebf70e6dfdd0d9f350548cbc175e29c533138f99272ad7767952258d0d30b2d749d41cafd0234aaa094dd2189c49f6568b4c001dd52d8ad6b63c724f8

5.4 HMAC-SHA-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)	19bd6999e03d0250ee5ae90a78429897fcaf7498c6a2fc44245ee4bd9455b19e 343ab44e98d97d8a75460126647579a1c8b4d9ce796f38688acb1d03613f7dd3
3	K(2)	59a3df3109ce3dc95df83cba0e13d991ea48abd145025e942f1cf78dad4b62a9 f7aa0b532c64b5ddc233dd6db910c83664cb373b6ba3dbd5d4751c5284c9aa2f
4	K(n)	73aa82e6233b6a8a51b08441127e838700e4480ee8b5300cbad5fe48ba2a4ab1 d5cf45623ec4795b9429f57727228f8c789c144df34542206bd3852d786d0e6c
5	result(n)	19bd6999e03d0250ee5ae90a78429897fcaf7498c6a2fc44245ee4bd9455b19e 343ab44e98d97d8a75460126647579a1c8b4d9ce796f38688acb1d03613f7dd3 59a3df3109ce3dc95df83cba0e13d991ea48abd145025e942f1cf78dad4b62a9 f7aa0b532c64b5ddc233dd6db910c83664cb373b6ba3dbd5d4751c5284c9aa2f 73aa82e6233b6a8a51b08441127e838700e4480ee8b5300cbad5fe48ba2a4ab1 d5cf45623ec4795b9429f57727228f8c789c144df34542206bd3852d786d0e6c
6	K0	19bd6999e03d0250ee5ae90a78429897fcaf7498c6a2fc44245ee4bd9455b19e 343ab44e98d97d8a75460126647579a1c8b4d9ce796f38688acb1d03613f7dd3 59a3df3109ce3dc95df83cba0e13d991ea48abd145025e942f1cf78dad4b62a9 f7aa0b532c64b5ddc233dd6db910c83664cb373b6ba3dbd5d4751c5284c9aa2f 73aa82e6233b6a8a51b08441127e838700e4480ee8b5300cbad5fe48ba2a4ab1

6 피드백 모드를 이용한 키 유도 함수 참조 구현값



6.1 HMAC-SHA-224의 단계별 참조 구현값

6.1.1 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)	00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	fc211d4bbb65e20544617963fdab1f5217837ec583d45b4fb45208ff
3	K(2)	d56179c61dc5b54e04dbab27481706941cafe4565f89d40f16a6ce96
4	K(n)	d2d2f9d71b3aad54135b04c69c5e6541ebed6a58abf0fd2e0351701e
5	result(n)	fc211d4bbb65e20544617963fdab1f5217837ec583d45b4fb45208ffd56179c61dc5b54e04dbab27481706941cafe4565f89d40f16a6ce96d2d2f9d71b3aad54135b04c69c5e6541ebed6a58abf0fd2e0351701e
6	K0	fc211d4bbb65e20544617963fdab1f5217837ec583d45b4fb45208ffd56179c61dc5b54e04dbab27481706941cafe4565f89d40f16a6ce96d2d2f9d71b3aad54135b04c69c5e

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)	e50dccef026d0d446f34c90f919bbff924cb57e09caa9ec30f05eaba
3	K(2)	66227939ddbc98fb6b066429c0b694399a21f42bad3445917ec5068b
4	K(n)	87b6f6c97145d096958594fb4bd46385c4fc6771cd4f2adc2af371a5
5	result(n)	e50dccef026d0d446f34c90f919bbff924cb57e09caa9ec30f05eaba66227939 ddbc98fb6b066429c0b694399a21f42bad3445917ec5068b87b6f6c97145d096 958594fb4bd46385c4fc6771cd4f2adc2af371a5
6	K0	e50dccef026d0d446f34c90f919bbff924cb57e09caa9ec30f05eaba66227939 ddbc98fb6b066429c0b694399a21f42bad3445917ec5068b87b6f6c97145d096 958594fb4bd4

6.1.3 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)	00112233445566778899aabbccddeeff00112233445566778899aabb
	L (16진수)	0230

위치	변수	중간값(16진수)
1	n	3
2	K(1)	08d1602aef799313203f31dee8296a72ada6da376a6433bc05981b40
3	K(2)	e80e72f8923290b616bc30fd96c3af7f133bbc9660bafbec2bcc656d
4	K(n)	2efaefb8c7b4da4d79d4d9f85c72df15fb356e692f38523d6f1a8ebb
5	result(n)	08d1602aef799313203f31dee8296a72ada6da376a6433bc05981b40e80e72f8923290b616bc30fd96c3af7f133bbc9660bafbec2bcc656d2efaefb8c7b4da4d79d4d9f85c72df15fb356e692f38523d6f1a8ebb
6	K0	08d1602aef799313203f31dee8296a72ada6da376a6433bc05981b40e80e72f8923290b616bc30fd96c3af7f133bbc9660bafbec2bcc656d2efaefb8c7b4da4d79d4d9f85c72

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)	d1ce68d860217fc020000127de74b7d0b8a83fd6212a014344683abf
3	K(2)	6e6f3681408fa8a8c0271b451d460487e645ee1cc3882c514b7e2c92
4	K(n)	cb3ec40f4a51538bac3d12905f561bd68f632a21ea6b0d40bef80f5e
5	result(n)	d1ce68d860217fc020000127de74b7d0b8a83fd6212a014344683abf6e6f3681408fa8a8c0271b451d460487e645ee1cc3882c514b7e2c92cb3ec40f4a51538bac3d12905f561bd68f632a21ea6b0d40bef80f5e
6	K0	d1ce68d860217fc020000127de74b7d0b8a83fd6212a014344683abf6e6f3681408fa8a8c0271b451d460487e645ee1cc3882c514b7e2c92cb3ec40f4a51538bac3d12905f56

6.2 HMAC-SHA-256의 단계별 참조 구현값

6.2.1 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)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	c976edededeabac660620a1bfb10f8f1471c445600d4b639de34cff39d7796f0a4
3	K(2)	147eb3426930257c2dd9990bdf95441f49f78bc03c6e63a2c306c32b46fac3af
4	K(n)	bae4ccf905d7fcc6127167fa77506709139c1bee54130178bda8809ced3f2c08
5	result(n)	c976edededeabac660620a1bfb10f8f1471c445600d4b639de34cff39d7796f0a4 147eb3426930257c2dd9990bdf95441f49f78bc03c6e63a2c306c32b46fac3af bae4ccf905d7fcc6127167fa77506709139c1bee54130178bda8809ced3f2c08
6	K0	c976edededeabac660620a1bfb10f8f1471c445600d4b639de34cff39d7796f0a4 147eb3426930257c2dd9990bdf95441f49f78bc03c6e63a2c306c32b46fac3af bae4ccf905d7fcc6127167fa77506709

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)	8da6974e8e8683042d73b24239658e7e2cef712e9335059cd34d5b2f8a25e9c9
3	K(2)	0e905156c6141095efe48d6d797c51a5fe3a51202a99390697294d3f784c8388
4	K(n)	e3da32cb27d3ac2b32eaca99b971c2f0f3e00ac8fa5de2e2909d934430222476
5	result(n)	8da6974e8e8683042d73b24239658e7e2cef712e9335059cd34d5b2f8a25e9c9 0e905156c6141095efe48d6d797c51a5fe3a51202a99390697294d3f784c8388 e3da32cb27d3ac2b32eaca99b971c2f0f3e00ac8fa5de2e2909d934430222476
6	K0	8da6974e8e8683042d73b24239658e7e2cef712e9335059cd34d5b2f8a25e9c9 0e905156c6141095efe48d6d797c51a5fe3a51202a99390697294d3f784c8388 e3da32cb27d3ac2b32eaca99b971c2f0

6.2.3 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)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0280

위치	변수	중간값(16진수)
1	n	3
2	K(1)	0dec972f54944b77c2bc3d54ba89e2d513c4a1226a738631f14fec1f919ed7f1
3	K(2)	2e98d548a0e293238a7dc423d3bc8f92bc5253b59904709732817730939e6e12
4	K(n)	25ca8a6c45ee39c2b65a146d7bc8d36a27072588787b724cbd9052cd5f3e65c0
5	result(n)	0dec972f54944b77c2bc3d54ba89e2d513c4a1226a738631f14fec1f919ed7f1 2e98d548a0e293238a7dc423d3bc8f92bc5253b59904709732817730939e6e12 25ca8a6c45ee39c2b65a146d7bc8d36a27072588787b724cbd9052cd5f3e65c0
6	K0	0dec972f54944b77c2bc3d54ba89e2d513c4a1226a738631f14fec1f919ed7f1 2e98d548a0e293238a7dc423d3bc8f92bc5253b59904709732817730939e6e12 25ca8a6c45ee39c2b65a146d7bc8d36a

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)	8005439e7f5d28f81d1fe0f640b5d6dfafa8e9266bcc248ad6197280c8a65f1b
3	K(2)	d22a07b187c697ff56190d7bf61ea5c6d2217abd3a114a643d6ffe9259c50db2
4	K(n)	fcb17fb72b29463293a580f394ca3c9d91d01f7fccfdb68b3ce264d08ade5e98
5	result(n)	8005439e7f5d28f81d1fe0f640b5d6dfafa8e9266bcc248ad6197280c8a65f1b d22a07b187c697ff56190d7bf61ea5c6d2217abd3a114a643d6ffe9259c50db2 fcb17fb72b29463293a580f394ca3c9d91d01f7fccfdb68b3ce264d08ade5e98
6	K0	8005439e7f5d28f81d1fe0f640b5d6dfafa8e9266bcc248ad6197280c8a65f1b d22a07b187c697ff56190d7bf61ea5c6d2217abd3a114a643d6ffe9259c50db2 fcb17fb72b29463293a580f394ca3c9d

6.3 HMAC-SHA-384의 단계별 참조 구현값

6.3.1 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)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	69ae00a7556ecec8769493b4937a473e25a322a0f9e9a68326ddb0ce512c5cf0 b4dd7823ede1d4ee45cdee7bc5e5a347
3	K(2)	69aee0fb17194af45d2edfd6b9f6e87f3f13419efe31a965c20284b5c956b4a0 ac14f24b479d589556f5e10a3dfd6fa8
4	K(n)	bd2d93fcdc02585eafc055f3db4446873add76fc465cf4eabbd48a02dbf31f1f 63db35a969042087da9f7db423d58546
5	result(n)	69ae00a7556ecec8769493b4937a473e25a322a0f9e9a68326ddb0ce512c5cf0 b4dd7823ede1d4ee45cdee7bc5e5a34769aee0fb17194af45d2edfd6b9f6e87f 3f13419efe31a965c20284b5c956b4a0ac14f24b479d589556f5e10a3dfd6fa8 bd2d93fcdc02585eafc055f3db4446873add76fc465cf4eabbd48a02dbf31f1f 63db35a969042087da9f7db423d58546
6	K0	69ae00a7556ecec8769493b4937a473e25a322a0f9e9a68326ddb0ce512c5cf0 b4dd7823ede1d4ee45cdee7bc5e5a34769aee0fb17194af45d2edfd6b9f6e87f 3f13419efe31a965c20284b5c956b4a0ac14f24b479d589556f5e10a3dfd6fa8 bd2d93fcdc02585eafc055f3db4446873add76fc465cf4ea

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)	aa66fcf02050a4a0ae12eb9a7be4263374fcd08127634e05d6afe4237d10a6e75042ab595d9b08d72bcbd11d5cf727e9
3	K(2)	b70d5096bd3fa298448355184bea1198b8213bd9a8fb485910209cd630115e4bd87c16898ee0d0b5f20da76fe1d82bf9
4	K(n)	e05118a3f8d5a1dc74ebbeaf401aac96394ccfdd425a2eeb967efd0a421c6fa3af783a77c36dcd0c33b474d98152ba9e
5	result(n)	aa66fcf02050a4a0ae12eb9a7be4263374fcd08127634e05d6afe4237d10a6e75042ab595d9b08d72bcbd11d5cf727e9b70d5096bd3fa298448355184bea1198b8213bd9a8fb485910209cd630115e4bd87c16898ee0d0b5f20da76fe1d82bf9e05118a3f8d5a1dc74ebbeaf401aac96394ccfdd425a2eeb967efd0a421c6fa3af783a77c36dcd0c33b474d98152ba9e
6	K0	aa66fcf02050a4a0ae12eb9a7be4263374fcd08127634e05d6afe4237d10a6e75042ab595d9b08d72bcbd11d5cf727e9b70d5096bd3fa298448355184bea1198b8213bd9a8fb485910209cd630115e4bd87c16898ee0d0b5f20da76fe1d82bf9e05118a3f8d5a1dc74ebbeaf401aac96394ccfdd425a2eeb

6.3.3 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)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	L (16진수)	03C0

위치	변수	중간값(16진수)
1	n	3
2	K(1)	612ca163396ec96b6ae094eaed548e1f649adce06300ab252705f65124ca63e9 eac39e5bbb3e440f62a5d2595cccebed
3	K(2)	80ebd68a337581817a4e1bd0c320ffe36ab83c29a415660e0e859fcf3e4c6eb2 107425a179263dcdd79cb97dbb810afa
4	K(n)	3b09a0cd2e1045f88666581da70294b0fc69032cd4c98fb3a8479a900971831e 2aaa5cf6d1989da27b8ca9b59e5ad8e7
5	result(n)	612ca163396ec96b6ae094eaed548e1f649adce06300ab252705f65124ca63e9 eac39e5bbb3e440f62a5d2595cccebed80ebd68a337581817a4e1bd0c320ffe3 6ab83c29a415660e0e859fcf3e4c6eb2107425a179263dcdd79cb97dbb810afa 3b09a0cd2e1045f88666581da70294b0fc69032cd4c98fb3a8479a900971831e 2aaa5cf6d1989da27b8ca9b59e5ad8e7
6	K0	612ca163396ec96b6ae094eaed548e1f649adce06300ab252705f65124ca63e9 eac39e5bbb3e440f62a5d2595cccebed80ebd68a337581817a4e1bd0c320ffe3 6ab83c29a415660e0e859fcf3e4c6eb2107425a179263dcdd79cb97dbb810afa 3b09a0cd2e1045f88666581da70294b0fc69032cd4c98fb3

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)	4011a8396cf4caa2aedc8e7ad400641e94af29cc98d6be574203db5b1276dab20cccedca5a6f4678eeefdf5effe0d05f
3	K(2)	f622a6303e4eeea0fc3e9c6dc3349fc7ecbaab0de9b069e3448f80d49f9cd0d707ccd6fa5a8acdb84b4a5b47f5adf387
4	K(n)	698c3ac63e07d18c589a880093c4bd28355a7a656b2f649326ba0e46ad6905a4bed6933a489b2bc681b4312a212cd80d
5	result(n)	4011a8396cf4caa2aedc8e7ad400641e94af29cc98d6be574203db5b1276dab20cccedca5a6f4678eeefdf5effe0d05ff622a6303e4eeea0fc3e9c6dc3349fc7ecbaab0de9b069e3448f80d49f9cd0d707ccd6fa5a8acdb84b4a5b47f5adf387698c3ac63e07d18c589a880093c4bd28355a7a656b2f649326ba0e46ad6905a4bed6933a489b2bc681b4312a212cd80d
6	K0	4011a8396cf4caa2aedc8e7ad400641e94af29cc98d6be574203db5b1276dab20cccedca5a6f4678eeefdf5effe0d05ff622a6303e4eeea0fc3e9c6dc3349fc7ecbaab0de9b069e3448f80d49f9cd0d707ccd6fa5a8acdb84b4a5b47f5adf387698c3ac63e07d18c589a880093c4bd28355a7a656b2f6493

6.4 HMAC-SHA-512의 단계별 참조 구현값

6.4.1 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)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	833fa5ecd02726858d6486bf3a93429b0d2f3882d791b26434121e7de50a6641 4707625fcd0067390f4ead1ab4e511d62f479aaef7aa22e3876ed3ee9866e740
3	K(2)	5b6cf435bbd313dbea90752d495859f40209e38dac39bfa2d9bdd28a70db4db0 829304d75c7c62c792e87a728832a91eb67d0b5d56e3c7a972a6cb5388610899
4	K(n)	306c36630ee1a80c886e45eb8131884b0c02b914b8ab847917b8407b8d029408 9efa435bb5648e7088216233125401936e876e80f8a365f2c30f80be8c6f6c96
5	result(n)	833fa5ecd02726858d6486bf3a93429b0d2f3882d791b26434121e7de50a6641 4707625fcd0067390f4ead1ab4e511d62f479aaef7aa22e3876ed3ee9866e740 5b6cf435bbd313dbea90752d495859f40209e38dac39bfa2d9bdd28a70db4db0 829304d75c7c62c792e87a728832a91eb67d0b5d56e3c7a972a6cb5388610899 306c36630ee1a80c886e45eb8131884b0c02b914b8ab847917b8407b8d029408 9efa435bb5648e7088216233125401936e876e80f8a365f2c30f80be8c6f6c96
6	K0	833fa5ecd02726858d6486bf3a93429b0d2f3882d791b26434121e7de50a6641 4707625fcd0067390f4ead1ab4e511d62f479aaef7aa22e3876ed3ee9866e740 5b6cf435bbd313dbea90752d495859f40209e38dac39bfa2d9bdd28a70db4db0 829304d75c7c62c792e87a728832a91eb67d0b5d56e3c7a972a6cb5388610899 306c36630ee1a80c886e45eb8131884b0c02b914b8ab847917b8407b8d029408

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)	19bd6999e03d0250ee5ae90a78429897fcaf7498c6a2fc44245ee4bd9455b19e 343ab44e98d97d8a75460126647579a1c8b4d9ce796f38688acb1d03613f7dd3
3	K(2)	a91e9a8953e9593a2ea6d8a6311e0e80bcf3d6dd81fc1b9230e657464df9997d 032a76725d868b6ded739a70e273e5c29fe922a03200371d3e587c2dcfd7a020
4	K(n)	83746b74c09591995ed75e917ebd77532e5d0da75416a668d76ee6b877d05bc5 02f4a54273c79431b34ab2cd623e7795f7ca67abada213952f7a4646dba6c580
5	result(n)	19bd6999e03d0250ee5ae90a78429897fcaf7498c6a2fc44245ee4bd9455b19e 343ab44e98d97d8a75460126647579a1c8b4d9ce796f38688acb1d03613f7dd3 a91e9a8953e9593a2ea6d8a6311e0e80bcf3d6dd81fc1b9230e657464df9997d 032a76725d868b6ded739a70e273e5c29fe922a03200371d3e587c2dcfd7a020 83746b74c09591995ed75e917ebd77532e5d0da75416a668d76ee6b877d05bc5 02f4a54273c79431b34ab2cd623e7795f7ca67abada213952f7a4646dba6c580
6	K0	19bd6999e03d0250ee5ae90a78429897fcaf7498c6a2fc44245ee4bd9455b19e 343ab44e98d97d8a75460126647579a1c8b4d9ce796f38688acb1d03613f7dd3 a91e9a8953e9593a2ea6d8a6311e0e80bcf3d6dd81fc1b9230e657464df9997d 032a76725d868b6ded739a70e273e5c29fe922a03200371d3e587c2dcfd7a020 83746b74c09591995ed75e917ebd77532e5d0da75416a668d76ee6b877d05bc5

6.4.3 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)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	L (16진수)	0500

위치	변수	중간값(16진수)
1	n	3
2	K(1)	2ddd5c4ae498189e38318472306347206e4ef9cb5447c605a0104b054922b13d 2e2e8b98a10eed328a208b3e4bc27a68f397d5a28e8d10d8b7c1f402c90f2504
3	K(2)	89179d8617a963b6e4f1499888beb7d794535c2366376f7ecd86e7d779528aef ca7f926befd98e5d1951af5a157c25f7c9d3a0c08bbb85ac30995732dd13ae4a
4	K(n)	b9fd332c98a7908ccffec6e9574b45a5284bff4f68a96618c4fa88e95c29e39d b7f27fe30fe098146f2ec535863524640d35d1fd2407005f1db70cc3cab127be
5	result(n)	2ddd5c4ae498189e38318472306347206e4ef9cb5447c605a0104b054922b13d 2e2e8b98a10eed328a208b3e4bc27a68f397d5a28e8d10d8b7c1f402c90f2504 89179d8617a963b6e4f1499888beb7d794535c2366376f7ecd86e7d779528aef ca7f926befd98e5d1951af5a157c25f7c9d3a0c08bbb85ac30995732dd13ae4a b9fd332c98a7908ccffec6e9574b45a5284bff4f68a96618c4fa88e95c29e39d b7f27fe30fe098146f2ec535863524640d35d1fd2407005f1db70cc3cab127be
6	K0	2ddd5c4ae498189e38318472306347206e4ef9cb5447c605a0104b054922b13d 2e2e8b98a10eed328a208b3e4bc27a68f397d5a28e8d10d8b7c1f402c90f2504 89179d8617a963b6e4f1499888beb7d794535c2366376f7ecd86e7d779528aef ca7f926befd98e5d1951af5a157c25f7c9d3a0c08bbb85ac30995732dd13ae4a b9fd332c98a7908ccffec6e9574b45a5284bff4f68a96618c4fa88e95c29e39d

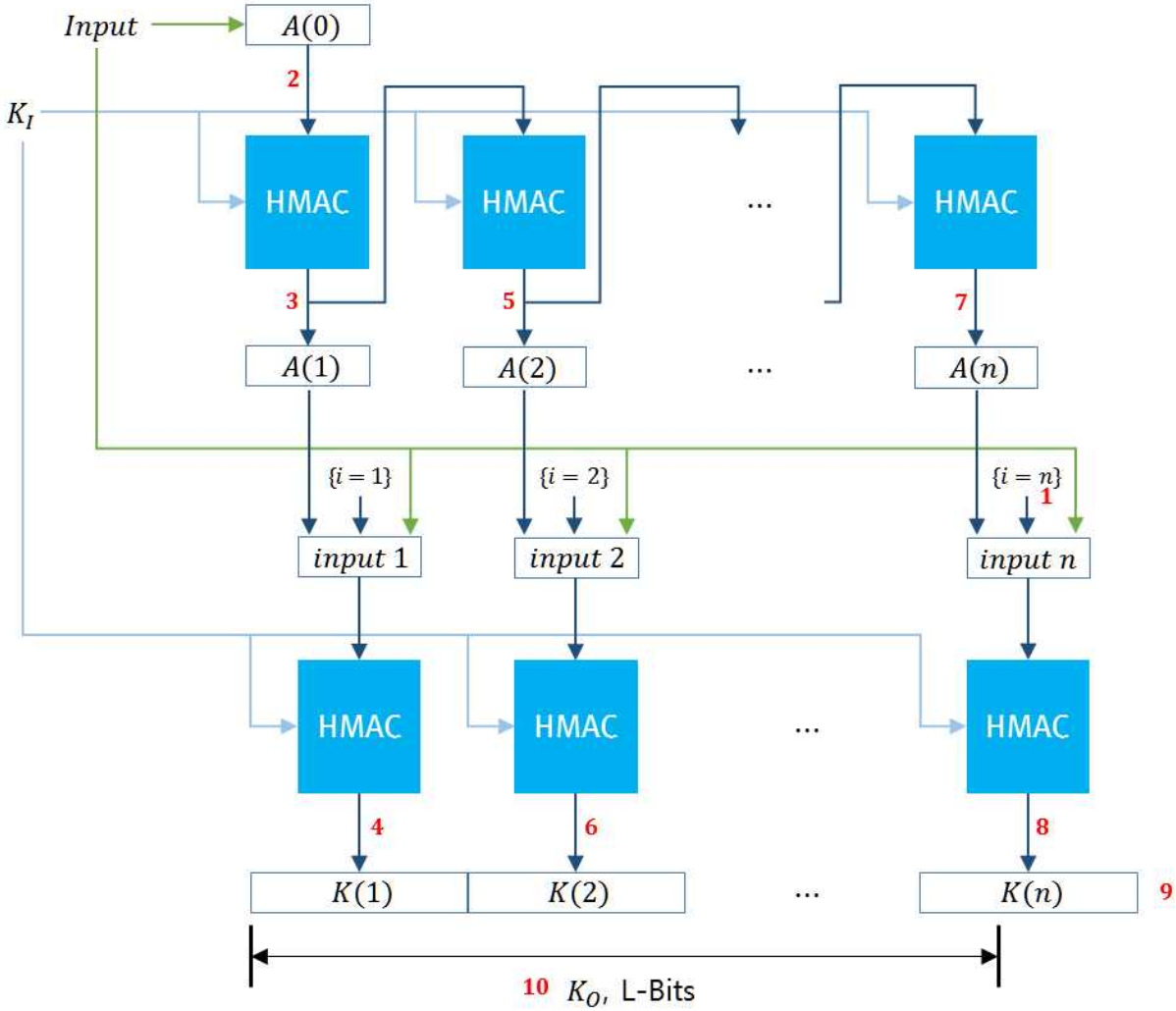
6.4.4 카운터 입력을 사용하지 않고 IV = ∅인 경우

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)	b78b6c62a332158347e6afb027d1d74ff47a35b5e75aa0a52f5bce12aedc3720 91063e61e4fa73c05db78211b572fc7821abc8e473dc1cbed34471ec32a4ee9c
3	K(2)	ad519e1bcb7dad930fe966ac6e3a0d410afeadcf0ee812639043027db76723e9 d7a2695653c61283fe33bafbbec85d9263d50c6911e1a16932c0d65afbbc6001
4	K(n)	e760fd3c41090f06aa2259924f5da09a16f6bb9cfd86e2c27d406b1a64c233c2 94233896563cbde0f43c69d70f6d2df18e467ca0bdbc8db1dd62659872800861
5	result(n)	b78b6c62a332158347e6afb027d1d74ff47a35b5e75aa0a52f5bce12aedc3720 91063e61e4fa73c05db78211b572fc7821abc8e473dc1cbed34471ec32a4ee9c ad519e1bcb7dad930fe966ac6e3a0d410afeadcf0ee812639043027db76723e9 d7a2695653c61283fe33bafbbec85d9263d50c6911e1a16932c0d65afbbc6001 e760fd3c41090f06aa2259924f5da09a16f6bb9cfd86e2c27d406b1a64c233c2 94233896563cbde0f43c69d70f6d2df18e467ca0bdbc8db1dd62659872800861
6	K0	b78b6c62a332158347e6afb027d1d74ff47a35b5e75aa0a52f5bce12aedc3720 91063e61e4fa73c05db78211b572fc7821abc8e473dc1cbed34471ec32a4ee9c ad519e1bcb7dad930fe966ac6e3a0d410afeadcf0ee812639043027db76723e9 d7a2695653c61283fe33bafbbec85d9263d50c6911e1a16932c0d65afbbc6001 e760fd3c41090f06aa2259924f5da09a16f6bb9cfd86e2c27d406b1a64c233c2

7 더블-파이프라인 반복 모드를 이용한 키 유도 함수 참조 구현값

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



7.1 HMAC-SHA-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)	d1ce68d860217fc020000127de74b7d0b8a83fd6212a014344683abf
4	K(1)	91e89383285b9691d38d0f0833cac5a030cc6a51741753e26b5f042f
5	A(2)	3c79f2ff6921201d27cf2ef5df2b65359ef5c305e486a56b21b21c4d
6	K(2)	2687b69e972feaeaf6d4732353fd6095e56e0aa338ad361c24df78b3
7	A(n)	f0eeb7006b0b3e9c1146f64e2468da8cb94275562a2eb57082667cae
8	K(n)	7f6503437debf14ceda8efa84c9a90d947cc3c9e33c0953b373ef0c2
9	result(n)	91e89383285b9691d38d0f0833cac5a030cc6a51741753e26b5f042f2687b69e 972feaeaf6d4732353fd6095e56e0aa338ad361c24df78b37f6503437debf14c eda8efa84c9a90d947cc3c9e33c0953b373ef0c2
10	K0	91e89383285b9691d38d0f0833cac5a030cc6a51741753e26b5f042f2687b69e 972feaeaf6d4732353fd6095e56e0aa338ad361c24df78b37f6503437debf14c eda8efa84c9a

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)	d1ce68d860217fc020000127de74b7d0b8a83fd6212a014344683abf
4	K(1)	6e6f3681408fa8a8c0271b451d460487e645ee1cc3882c514b7e2c92
5	A(2)	3c79f2ff6921201d27cf2ef5df2b65359ef5c305e486a56b21b21c4d
6	K(2)	fede6faf07ccf39fba75fc19f5a5b6035b6bd49bebc8fb5caf39e4c3
7	A(n)	f0eeb7006b0b3e9c1146f64e2468da8cb94275562a2eb57082667cae
8	K(n)	7df1788b63485a1956d5c395c14eb2db652c8878e1355fc8c2160295
9	result(n)	6e6f3681408fa8a8c0271b451d460487e645ee1cc3882c514b7e2c92fede6faf 07ccf39fba75fc19f5a5b6035b6bd49bebc8fb5caf39e4c37df1788b63485a19 56d5c395c14eb2db652c8878e1355fc8c2160295
10	K0	6e6f3681408fa8a8c0271b451d460487e645ee1cc3882c514b7e2c92fede6faf 07ccf39fba75fc19f5a5b6035b6bd49bebc8fb5caf39e4c37df1788b63485a19 56d5c395c14e

7.2 HMAC-SHA-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)	8005439e7f5d28f81d1fe0f640b5d6dfafa8e9266bcc248ad6197280c8a65f1b
4	K(1)	87fbdd5fa8238f98deee8715a6987b33db68ee2807b289a0f42fe99350784f9c
5	A(2)	13288051411e87d3009f1cc76f2130b1c3c9f21ad72c64713786fa0195318812
6	K(2)	7899174abc221c4d2dcd21d850332223ca01b827324ae506c8ef58fa165a2353
7	A(n)	593803ccd9dce3c17b8324ece4c121e7bdd76f991b82b38e20cd79a01adcf48b
8	K(n)	4f998ed2dfea25a935f964e14831cabc7ea926896839897 1aa8e4ba79157694e
9	result(n)	87fbdd5fa8238f98deee8715a6987b33db68ee2807b289a0f42fe99350784f9c 7899174abc221c4d2dcd21d850332223ca01b827324ae506c8ef58fa165a2353 4f998ed2dfea25a935f964e14831cabc7ea926896839897 1aa8e4ba79157694e
10	K0	87fbdd5fa8238f98deee8715a6987b33db68ee2807b289a0f42fe99350784f9c 7899174abc221c4d2dcd21d850332223ca01b827324ae506c8ef58fa165a2353 4f998ed2dfea25a935f964e14831cabc

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)	8005439e7f5d28f81d1fe0f640b5d6dfafa8e9266bcc248ad6197280c8a65f1b
4	K(1)	d22a07b187c697ff56190d7bf61ea5c6d2217abd3a114a643d6ffe9259c50db2
5	A(2)	13288051411e87d3009f1cc76f2130b1c3c9f21ad72c64713786fa0195318812
6	K(2)	a62327c9f79a5b723b3ed727aadc58470fa473d3171d02ecd2c8017b4ba48fd6
7	A(n)	593803ccd9dce3c17b8324ece4c121e7bdd76f991b82b38e20cd79a01adcf48b
8	K(n)	edfcc08ca9a3197aad5f19591f0c481259e74e1cca8882524b0f0be4d751a7ec
9	result(n)	d22a07b187c697ff56190d7bf61ea5c6d2217abd3a114a643d6ffe9259c50db2 a62327c9f79a5b723b3ed727aadc58470fa473d3171d02ecd2c8017b4ba48fd6 edfcc08ca9a3197aad5f19591f0c481259e74e1cca8882524b0f0be4d751a7ec
10	K0	d22a07b187c697ff56190d7bf61ea5c6d2217abd3a114a643d6ffe9259c50db2 a62327c9f79a5b723b3ed727aadc58470fa473d3171d02ecd2c8017b4ba48fd6 edfcc08ca9a3197aad5f19591f0c4812

7.3 HMAC-SHA-384의 단계별 참조 구현값

7.3.1 카운터 입력을 사용한 경우

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	A(0)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabb00001122 33445566778899aabbccddeeff00112233445566778899aabbccddeeff001122 33445566778899aabbccddeeff00112233445566778899aabb03c0
3	A(1)	4011a8396cf4caa2aedc8e7ad400641e94af29cc98d6be574203db5b1276dab2 0cccedca5a6f4678eeefdf5effe0d05f
4	K(1)	d4cf1159dbf331b40985a160531d73f2166303ca0bb46ad717e9207cd36a29f4 2eb748490e94e07596ae3a1f099f928a
5	A(2)	ffa8567be7e70e8af854dfe893ef7518e9c793bed4099276eab7dcd894f01c01 642eabbac0219eb0b048e3bfb1205c74
6	K(2)	78e27a472f7d9bd0965220846f2367af5c8e16c9d680841a5b02e5fcbf65d70d c82cfd3c6d7589536a24ac5342529359
7	A(n)	ff9b5de40f2bc981c594732c920055b49c61cb5986fba7155d9484d03d7d47d0 71865a97f9aab6073859386327b8ca83
8	K(n)	c13536d6b440a652d0c62d13a3411f26495dfc680ac55fd4f10d5a1b6a2a5834 c9d9d37908fd4a9646f70a4c91d1dd32
9	result(n)	d4cf1159dbf331b40985a160531d73f2166303ca0bb46ad717e9207cd36a29f4 2eb748490e94e07596ae3a1f099f928a78e27a472f7d9bd0965220846f2367af 5c8e16c9d680841a5b02e5fcbf65d70dc82cfd3c6d7589536a24ac5342529359 c13536d6b440a652d0c62d13a3411f26495dfc680ac55fd4f10d5a1b6a2a5834 c9d9d37908fd4a9646f70a4c91d1dd32
10	K0	d4cf1159dbf331b40985a160531d73f2166303ca0bb46ad717e9207cd36a29f4 2eb748490e94e07596ae3a1f099f928a78e27a472f7d9bd0965220846f2367af 5c8e16c9d680841a5b02e5fcbf65d70dc82cfd3c6d7589536a24ac5342529359 c13536d6b440a652d0c62d13a3411f26495dfc680ac55fd4

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)	4011a8396cf4caa2aedc8e7ad400641e94af29cc98d6be574203db5b1276dab2 0cccedca5a6f4678eeefdf5effe0d05f
4	K(1)	f622a6303e4eeea0fc3e9c6dc3349fc7ecbaab0de9b069e3448f80d49f9cd0d7 07ccd6fa5a8acdb84b4a5b47f5adf387
5	A(2)	ffa8567be7e70e8af854dfe893ef7518e9c793bed4099276eab7dcd894f01c01 642eabbac0219eb0b048e3bfb1205c74
6	K(2)	a048db4855c63f8a8d6a1b5d7c4c730535cbc6a647f291cc0c66870c1e01cc7a 3cac9b07553da694b54ab2363d7972fd
7	A(n)	ff9b5de40f2bc981c594732c920055b49c61cb5986fba7155d9484d03d7d47d0 71865a97f9aab6073859386327b8ca83
8	K(n)	bf7ce73488ebf9045d5e978ceb1490e433f82dbe915fe223c7c7c3e157056846 d615fa19b774655dbd53c21789459713
9	result(n)	f622a6303e4eeea0fc3e9c6dc3349fc7ecbaab0de9b069e3448f80d49f9cd0d7 07ccd6fa5a8acdb84b4a5b47f5adf387a048db4855c63f8a8d6a1b5d7c4c7305 35cbc6a647f291cc0c66870c1e01cc7a3cac9b07553da694b54ab2363d7972fd bf7ce73488ebf9045d5e978ceb1490e433f82dbe915fe223c7c7c3e157056846 d615fa19b774655dbd53c21789459713
10	K0	f622a6303e4eeea0fc3e9c6dc3349fc7ecbaab0de9b069e3448f80d49f9cd0d7 07ccd6fa5a8acdb84b4a5b47f5adf387a048db4855c63f8a8d6a1b5d7c4c7305 35cbc6a647f291cc0c66870c1e01cc7a3cac9b07553da694b54ab2363d7972fd bf7ce73488ebf9045d5e978ceb1490e433f82dbe915fe223

7.4 HMAC-SHA-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)	b78b6c62a332158347e6afb027d1d74ff47a35b5e75aa0a52f5bce12aedc3720 91063e61e4fa73c05db78211b572fc7821abc8e473dc1cbed34471ec32a4ee9c
4	K(1)	d3a6779fd531ff6f327ec70f26d1f54798c867e86eae28ae6ced773ba2382190 a8c72fb5c912c9f8a7f4a9cdf65928d133e28b71764c841959d7a1133c08fd65
5	A(2)	22160b07928cacd5ac6799553f2e9c37b99bfb791dd79208703037e8d319b2a6 a4d979b17dc33e3d862f166fb16c79a17065a88906cd270adaaf7578cf84f40e
6	K(2)	df7ab5c457be9ce477ba71d3b54eb5c4cd824216e5f3267f300c071045cd3689 37f0e730328b364a6ae0a8e9a80ddac6430dc02247408e3b97a6a063502be9b0
7	A(n)	aa7d64ee1e2c732d2f1af96e8e689bed45809d62f79277c76ada66672ffa6d14 5104cf130cbe2a647d3df98216191529d1c1930849f16956f57e73acaaf911e3
8	K(n)	f52e2742021aab1f651b7063b25876310c0027bcf36ea9b4d577d9fc51f88b64 972345507513ac8060a005cbd7caada7b09f3820b5e22bfec442fdfaf1e6d8e5
9	result(n)	d3a6779fd531ff6f327ec70f26d1f54798c867e86eae28ae6ced773ba2382190 a8c72fb5c912c9f8a7f4a9cdf65928d133e28b71764c841959d7a1133c08fd65 df7ab5c457be9ce477ba71d3b54eb5c4cd824216e5f3267f300c071045cd3689 37f0e730328b364a6ae0a8e9a80ddac6430dc02247408e3b97a6a063502be9b0 f52e2742021aab1f651b7063b25876310c0027bcf36ea9b4d577d9fc51f88b64 972345507513ac8060a005cbd7caada7b09f3820b5e22bfec442fdfaf1e6d8e5
10	K0	d3a6779fd531ff6f327ec70f26d1f54798c867e86eae28ae6ced773ba2382190 a8c72fb5c912c9f8a7f4a9cdf65928d133e28b71764c841959d7a1133c08fd65 df7ab5c457be9ce477ba71d3b54eb5c4cd824216e5f3267f300c071045cd3689 37f0e730328b364a6ae0a8e9a80ddac6430dc02247408e3b97a6a063502be9b0 f52e2742021aab1f651b7063b25876310c0027bcf36ea9b4d577d9fc51f88b64

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)	b78b6c62a332158347e6afb027d1d74ff47a35b5e75aa0a52f5bce12aedc3720 91063e61e4fa73c05db78211b572fc7821abc8e473dc1cbed34471ec32a4ee9c
4	K(1)	ad519e1bcb7dad930fe966ac6e3a0d410afeadcf0ee812639043027db76723e9 d7a2695653c61283fe33bafbbec85d9263d50c6911e1a16932c0d65afbbc6001
5	A(2)	22160b07928cacd5ac6799553f2e9c37b99bfb791dd79208703037e8d319b2a6 a4d979b17dc33e3d862f166fb16c79a17065a88906cd270adaaf7578cf84f40e
6	K(2)	7dbd12e3ff6b1aa617894cca40b5d3d168daed59d4c41a2464cbfc2d3b9408a1 71b5e7e14128ffdd9f9f4cc760907e8ed7a8cfdd3515f7d90ce5cb2c57e0fe19
7	A(n)	aa7d64ee1e2c732d2f1af96e8e689bed45809d62f79277c76ada66672ffa6d14 5104cf130cbe2a647d3df98216191529d1c1930849f16956f57e73acaaf911e3
8	K(n)	eaeb52a4ebb7a4ab25ac273dfb078f413dda8f65f81b8c7fb9aaebad8e36cc3d a892169b33f83d75d4e8c0508d8c534ed53049f1dea5e378520889954c395ab7
9	result(n)	ad519e1bcb7dad930fe966ac6e3a0d410afeadcf0ee812639043027db76723e9 d7a2695653c61283fe33bafbbec85d9263d50c6911e1a16932c0d65afbbc6001 7dbd12e3ff6b1aa617894cca40b5d3d168daed59d4c41a2464cbfc2d3b9408a1 71b5e7e14128ffdd9f9f4cc760907e8ed7a8cfdd3515f7d90ce5cb2c57e0fe19 eaeb52a4ebb7a4ab25ac273dfb078f413dda8f65f81b8c7fb9aaebad8e36cc3d a892169b33f83d75d4e8c0508d8c534ed53049f1dea5e378520889954c395ab7
10	K0	ad519e1bcb7dad930fe966ac6e3a0d410afeadcf0ee812639043027db76723e9 d7a2695653c61283fe33bafbbec85d9263d50c6911e1a16932c0d65afbbc6001 7dbd12e3ff6b1aa617894cca40b5d3d168daed59d4c41a2464cbfc2d3b9408a1 71b5e7e14128ffdd9f9f4cc760907e8ed7a8cfdd3515f7d90ce5cb2c57e0fe19 eaeb52a4ebb7a4ab25ac273dfb078f413dda8f65f81b8c7fb9aaebad8e36cc3d

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

[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)