TTA Standard

정보통신단체표준(국문표준)

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

HMAC 기반 결정론적 난수발생기 - 제3부: 해시 함수 LSH

Deterministic Random Bit Generator based on HMAC - 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-Part3
표준 초안 작성자	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part3
	김동민	NSR	연구원	-	TTAK.KO-12.xxxx-Part3
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 LSH를 사용하는 HMAC(LSH) 기반의 DRBG 메커니즘 HMAC_DRBG의 참조 구현값을 제시하여, HMAC_DRBG의 구현 정확성을 확인할 수 있도록 한다.

2 주요 내용 요약

이 표준은 HMAC_DRBG 운용을 위해 고려할 수 있는 다양한 선택 요소(예측내성 활성화 여부, 시드별 출력 값 생성 횟수(reseed_interval), 개별화 문자열 입력 여부, 추가 입력 사용 여부)를 반영하여, LSH를 사용하는 HMAC_DRBG의 참조 구현값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 제1부 일반에 규정된 DRBG 메커니즘인 HMAC_DRBG의 기반 함수인 HMAC에 ISO/IEC 9797-2에 규정된 해시 함수 LSH를 적용한 결과로, HMAC_DRBG와 HMAC, 그리고 LSH는 각 표준의 상세 규격을 준용한다

3.2 인용 표준과 본 표준의 비교표

- 해당없음

Preface

1 Purpose

The standard provides test vectors of the DRBG mechanism, HMAC_DRBG, used as a hash function based on HMAC(LSH) about implementation conformance.

2 Summary

The standard specifies the test vectors of HMAC_DRBG used as HMAC(LSH) about implementation conformance. The standard reflects the various options (prediction resistance, reseed interval, personlization string, additional input) that can be considered for HMAC_DRBG operation.

3 Relationship to Reference Standards

The test vectors in this standard are result of applying the hash function LSH specified in ISO/IEC 9797-2 as the HMAC based on HMAC_DRBG, the DRBG mechanism specified in Part 1: General.
And, HMAC_DRBG, HMAC and LSH conform to the specifications of each standard.

목 차

HMAC 기반 결정론적 난수발생기
- 제3부: 해시 함수 LSH
(Deterministic Random Bit Generator based on HMAC
- Part3: Hash Function LSH)

1 적용 범위

이 표준은 해시 기반 메시지 인증 코드 HMAC(LSH)를 기반으로 동작하는 DRBG 메커니즘 HMAC_DRBG의 참조 구현값을 제시한다. HMAC_DRBG는 운용을 위한 다양한 선택 요소가 존재한다. 참조 구현값 생성을 위해 고려한 선택 요소는 다음과 같다.

- 예측내성 지원 여부
- 상태갱신 주기(reseed_interval) 설정
- 개별화 문자열 입력(personlization_string) 사용 여부
- 추가 입력(additional_input) 사용 여부

예측내성 지원과 상태갱신 주기는 생성 함수(generate function) 동작 과정에서 리씨드 함수(reseeding function)의 동작을 결정하는 요소이다. 그리고 개별화 문자열 입력과 추가 입력은 각각 인스턴스 생성 함수(instantiate function)와 리씨드 함수(generate function)에서 씨드 생성 과정과 출력값 생성에 영향을 미친다.

상태갱신 주기의 설정과 예측내성 지원 여부에 따른 리씨드 함수의 호출을 고려한 상세 시험 시나리오와 LSH를 기반 해시 함수로 사용한 참조 구현값은 5, 6, 7절에 기술어 있다. 시험 시나리오는 생성 함수의 리씨드 함수 호출 방식에 따른 동작을 위주로 다음과 같이 구분한다.

- 시나리오 1: 예측내성을 지원하지 않고 상태갱신 주기(reseed_interval)를 1로 설정
- 시나리오 2: 예측내성을 지원하지 않고 상태갱신 주기(reseed_interval)를 2로 설정
- 시나리오 3: 예측내성을 항상 지원

시나리오 1과 2는 예측내성을 지원하지 않는 경우이고 시나리오 3은 예측내성을 항상 지원한다. 이를 위해 시나리오 1과 2는 예측내성 활성화(*prediction_resistance_flag*) 파라미터와 예측내성 요구(*prediction_resistance_request*) 파라미터를 모두 0(unset)인 경우를 가정한다. 그리고 시나리오 1과 2는 출력 과정에서 리씨드 함수의 호출이 발생하는 경우와 아닌 경우를 구분한다. 따라서 시나리오 2는 리씨드 함수를 호출하지 않고 출력값을 생성하는 경우이고, 시나리오 1과 3은 출력값 생성 전 리씨드 함수를 호출한다.

개별 시험 시나리오에서 사용하는 공통 정보는 다음과 같다.

<표 1-1> HMAC_DRBG 난수발생기 입력값 정보

입력		값(16진수)
엔트로피 입력 (256 비트)	entropy_input 1 (entropy1)	7145910782ACCB48 308ABB1C0A410722 7B9F1AA8F26A6CD5 3F3C032741913A21
	entropy_input 2 (entropy2)	92BAA7658C23A7EE 8E80A8EECF3E2B68 91A52DFC49686515 007AC763F9244C8C
	entropy_input 3 (entropy3)	F148FD648C2B7BB0 9395FF218C07D367 B8CCE93A3B881F93 7E14C11DD2894FE6
논스 (128 비트)	nonce	BE1FC13D9266E528 0C87112E955995F3
개별화 문자열 (128 비트)	personalization_string (perString)	A1F6BEBDAF3ECD15 519841753BF5147D E010E9D693FD4C68 EC053ACD6EB1E405
추가 입력 (256 비트)	additional_input 1 (addInput1)	6625B06B16AF81E7 13A03866EC5B7B87 0CABB597E25A5DC0 3FFF7C7DFF176951
	additional_input 2 (addInput2)	EB57D7B9DE41125F 27F686902F4B81F0 5C1E3A6D34EB1171 C69A185C459BD331

- DRBG의 기반 해시 함수 알고리즘에 상관없이 <표 1-1>에 정의된 입력값을 사용한다. 단, DRBG 출력값의 비트 길이(requested_no_of_bits)는 해시 함수 알고리즘의 출력 길이의 2배로 설정한다. 예를 들어, LSH-256을 DRBG 내부 함수로 사용하는 경우 DRBG 출력값의 길이를 512 비트로 한다.

- DRBG 운용 주체에 의해 난수 생성이 2회 요청되었다고 가정한다. 따라서 LSH56을 사용하는 경우 512 비트를 2회 출력한다.

- 각 시나리오에서는 씨드 생성 과정과 출력값 생성에 영향을 미치는 선택 입력인 개별화 문자열과 추가 입력의 사용 여부에 따라 참조 구현값을 생성한다.

이 표준에서 다루는 세부 참조 구현값 생성 시나리오를 정리하면 <표 1-2>와 같다.

<표 1-2> 부가 입력 정보 설정에 따른 시험 분류

구분		예측내성	갱신 주기	개별화 문자열	추가 입력
(5절)시나리오 1 예측내성을 지원하지 않고 갱신주기를 1로 설정	5.2	X	1	0	0
	5.3	X	1	X	0
	5.4	X	1	0	X
	5.5	X	1	X	X
(6절)시나리오 2 예측내성을 지원하지 않고 갱신주기를 2로 설정	6.2	X	2	0	0
	6.3	X	2	X	0
	6.4	X	2	0	X
	6.5	X	2	X	X
(7절)시나리오 3 예측내성 항상 지원	7.2	0	-	0	0
	7.3	0	-	X	0
	7.4	0	-	0	X
	7.5	0	-	X	X

2 인용 표준

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

- TTAK.KO-12.0xxx-Part1, “해시 함수 기반 메시지인증코드 (HMAC) - 제1부: 일반”, 2018. 12.

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

3 용어 정의

- 해당없음

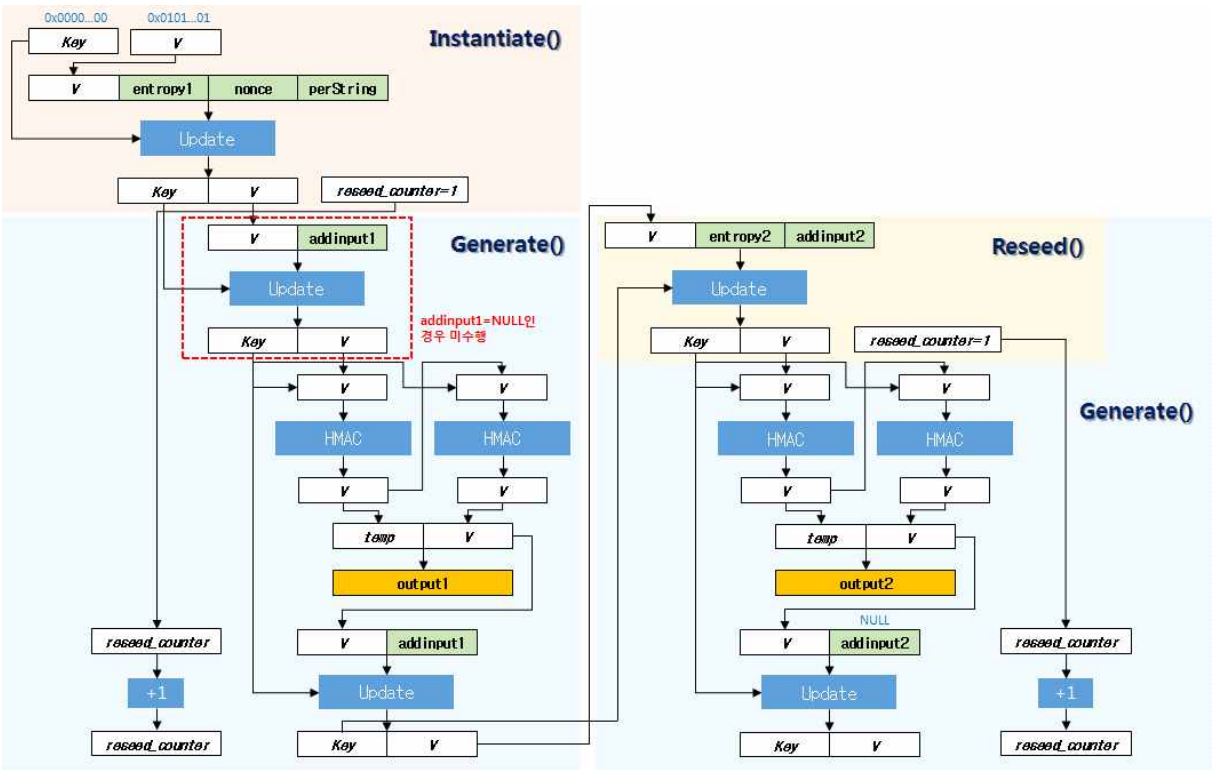
4 약어

- 해당없음

5 시나리오 1 (예측내성을 지원하지 않고 갱신주기를 1로 설정)

5.1 개요

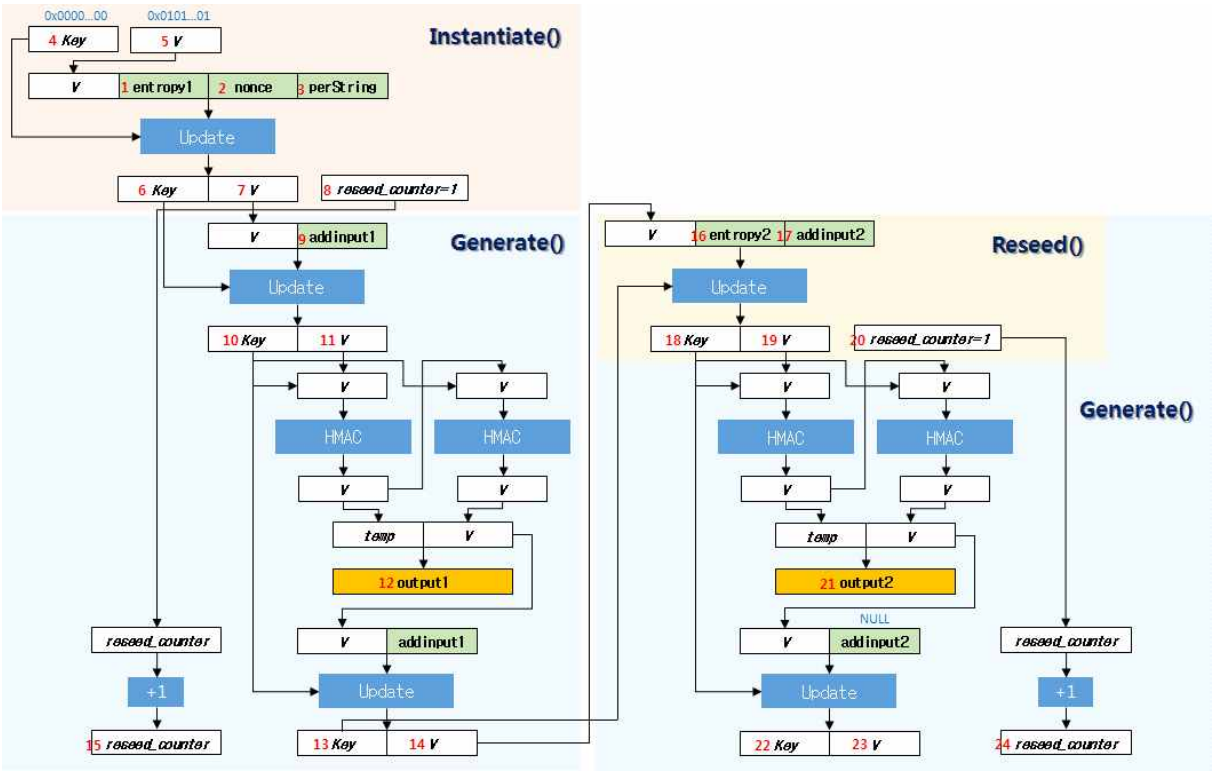
시나리오 1은 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 1로 설정할 경우의 HMAC_DRBG 참조 구현값을 제시한다. (그림 5-1)은 시나리오 1에 따른 HMAC_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 5-1) 예측내성을 지원하지 않고 상태갱신 주기가 1인 HMAC_DRBG 출력값 생성 과정

5.2 시나리오 1-1 (개별화 문자열 사용, 추가 입력 사용)

(그림 5-1)을 기준으로 참조 구현값 확인 위치를 도시하면 (그림 5-2)와 같다. 아래에서는 시나리오 1에서 개별화 문자열과 추가 입력을 모두 사용하는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.



(그림 5-2) 단계별 참조 구현값 위치

5.2.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	5527329894A1D3205839AA918031934AB3BB24E382B828E334789140
7	V	CF1F4580A206D2222974871186D8D2E3CCD6F3E04EE8B54948E4E754
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	6420C403615EF44A796D0F9F856B4A30E7E8754D0ECC48723B44F059

11	V	EEF8C4B33C85507F64A6A21611CAD58F7BF26A4E2C6838742556398E
12	output1	FEC95AAA45FF9D23093B44B6C7A104EC6E85ED7AD5C6650D1CDAD05F6EB8AF202F0D680B33D1C3E95AA1A9AD79BC343D47F24BDFBAD2EFC2
13	Key	61E711ED2E5AE44F1928F52F600418D274AF871B35192B0B2E4657B3
14	V	9247809F696656459F42770264FBF9D16AFEA9438C818C999E6FF54D
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
18	Key	FB9DF0BA056B647D90B889FCFB2E64A2425F16B57050AE449E597853
19	V	2D85AA5FEF534D9A0978B65EBDF307265FEE704B7AC170520AA9F894
20	reseed_counter	1
21	output2	7D7B0318EC5D7D24486FFD43BA28AB38ED232542B47F53E7E5809822AE785F846895BCE137BE08346E0C6A4DF95F7AC850FCA50908199FE8
22	Key	92FCBE66352F8FE8FFAED68EE546B529E87494778A0E0740FCFC958F
23	V	40DFC46B14529C5632BFFB75F346CDFEA0DB5E31FAE78726FAF0B182
24	reseed_counter	2

5.2.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	2FAD2936439B2CAED4A7C2831922BD532B43319DC8710E486A005B438F92B692
7	V	D9197497970B52B4B40FA99F208A5F2C5ADBC1056770144A29E8708C0474BDE2
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	1FD227D76FDBAC223F457C5436C0B12E8672BF5BFACEF680CAA577D036D06695
11	V	FC1091CABBFC11E90A795AB6324708C698CC8A81037442AB62E66089CDB9EACE
12	output1	1A679AB4513DEBB0BACD81F3E771727956DD4C8BABA15D8F1E197AE5DE4B85C82F6B01727B494F343DA06A6C5CBBB85D32C4DBC5D5AA64CAEDAD6A417D4AB0DD
13	Key	90D15019B8B9E9A3BEC53285ED757D0675902CC9D84598C1AB872AF8FCBF0EE9
14	V	98F0F75BEE8285D6ACFFB93AE26DF8F6303BA687A0D95F04A2EA0CF62606C334
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C

17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
18	Key	74BCC6F7B6309DD4FA21C39EFB56AF7F90A21EE5BC19380D1F17CECD77B3976D
19	V	D50986944F6DCFD665D495BF8B4A4F68D7CF7805A124E4BAF73C9E70CB4E44AD
20	reseed_counter	1
21	output2	ADADE2E9B97B6183100B8F32E6CE03AD79C8CE37F35440B4F77171844A808225 BAEE0ECBEBB36E2ED5C7C2B9751C452AF4126A1AB4A1263EC1558F45AE436CE3
22	Key	10599A7759BD107E2F523902F083DB914211C5440E610DDCA5A53CEDEA27A831
23	V	F09E2D551183A7B93F10E5A333C6082D732EB2F700467BA6F8803575E00C25D3
24	reseed_counter	2

5.2.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101 0101010101010101010101010101010101
6	Key	29CC03EF83F7577AE3C69F455776A27A6173CAB7E04412E8684367D52DC500A9 497ED86EE319700FDBEA3E87A7D6FD51
7	V	2D0CB4A09EAB51CB8A3177B0AF2F386B685306A21591F3E2C532FC9066857A72 19277BBD9C76CB315B78F76511325731
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	13AF35BE8E27D3BCC7212BB59BC4F3A87FBC7EF582E7D3E76B31CFE1258F70DD 2E7EB3F7F7FD2510449CCE6B3D993A82
11	V	42EA9E4E5604F8133A0BB1330F1A9F0AB714FEADC31B9EF50EB6DDF5E2597A74 63A7C0C92EAF6B7DE679AF6F90040827
12	output1	DFADB57F484AAE379BAA9E362285E955DD67C55EAF3ED1D485AB6789B528869B 3C17D6257A876E45DE80804620291DCF95AAD6DCCD5BEA1CC622C4D0589A5AD2 F986BC1825D6BDA70A84ADF17CB51321873E8BC19D0668757C4A12B33C4792EA
13	Key	B326B85DEA0E975F21B41ECC96AFDEE0C9575F8AFA27E15918FB65C2C184FDE5 607CA1CD93A4BE066D379BD05A312C67
14	V	7C359E33A4A899D4D9B19D15ECA2B09FB2FBF3687AB449C697D581446559B23C 640C3AAE986182A977B83225F25BE2E9
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331

18	Key	DF8B497D4222A737F17D890DA5C7FC6E0D3F774858560391022D53FF57190A00 AB6693AA1BBC351B3553B56935ABAB7B
19	V	52322D12E4AFCB0A8F5638CB5B1703240AAD63C2B4E7017784AE24BA53D5053B C3EC21BC764F5AAEEA934F0499141EE4
20	reseed_counter	1
21	output2	DC9BA8067C929B30CFDBDA42E87E3E1E1A63005784333DF1C3551BB50D9ADCCC 646A6A3DA87D737A78FA82B16BD177171DF0D1590BDB053D9EF6A9318647F087 847C3E12EE6D4AA4A1384C3977A97FFA452E46ED5E4A2572ADEA6944A3D5CC02
22	Key	8B53B3BF76EE4431A3EE0178D1C56E939F917F5BE9219ABAF1CFCADBA312F056 B5C0E317C8B7E45476A4AEB4C31C1E7B
23	V	A0216BE2DF1607B96B2A714282F832B2B6CA09FAFDF4AAB71EF9CB365FC12C71 850AB7593B4C36D4438D54FEA243B798
24	reseed_counter	2

5.2.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101 0101010101010101010101010101010101010101010101010101010101010101
6	Key	03CEEDF46432B9FAB1D8400BE97AFB38A8118B793EB9ECC00F3BE53163741EE5 B0EE7B5327697E26E0EE8D426AA1A8DB373F4A1D1B8402A141AF5C18685431EB
7	V	6BEF9B37F8265CCEF1B84CFB21284B8ECD9F4166B2FCB3E93B3A262BD9D0788D 5A4B236E808E125C5880591D545A73CBFCD9050C7E080789BEA38AD5F4C11432
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	BD109D3AF433D79016125D0431DFBC1EF610284FE8B963E7FF0D82EF0B0F4B82 24CC9599E15DDB04626A88797468937BAD603A6E33CDEFB95B1DDA5A6C111B6C
11	V	EAEB8EEC0F52DD57B2F48E2681AA182F4EFAE65EB28BD782DA1FA8AF1590BFCE 2E44861F82ECBEE1687C0F7740B301E0B250F386F6A05CB2C77B9F02FBCDA0CF
12	output1	4079EC4371DBB9635FCD8FE19D265811E0BC885B49570769F673D0487A6D2FC4 3C66F01974B90FE280C829349258C1B78A13BB134F426C45AB01A12AC96EE609 B7189A13CC2949917D31F95590E6856ACEB3DCE5C03586F5F75676C6C14E221E 4FC68F4A55331613FDAD5ABC85F12C4D25F92D69FCA446F6C7C9C44CAFBA997E
13	Key	338F51647751EEC121C6D61AFD4741632DAA1BC44EF780753AB6C844B808E73A 0016BCE6919B0775376236BFE70EF863A9557FBB52A18DB298BC4ACF4556317A
14	V	F34D765D27C977A697819F7D4DBA9833D060660898C86C3E2F229FBEC54FBD94 A82007B0D03D4A4B60D9CC7A6C62E17A91C65C06A16FC5F443D2FC66C3E9915C
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331

18	Key	E5F336DD0609340F19064721D8520FDC3EB152BE6BEDAB51C04BC193E29A708D A599F29766611B2885E5C97897E922D870800EC325314FD5B0A7E92FEB7E2EE3
19	V	500A0AB505D89632DE5865E5881370665FC5CC0E5273957B65A5C7933CACC56D 407B88864C41171948CBC90F1AF9F92E2CB1FDEC89FB5118D4BBE52E544176E5
20	reseed_counter	1
21	output2	811DFADF885C475191626B63BA50B881E2B52165ABCD2C7747A2E6B11D726859 8203CA1A04969BEA48278EAD59D07872D6E62B0A9EB4390570A5D75B8EE4B7E2 FAC8B21DF58505FBE87AF31701D72B84145A29550237024C76F54E219BAAF7F2 414536F52AA3570D9D1B7E69A8B127D9D67C6EA35BBFADC15A56B583168E8AF4
22	Key	FAE1BFCFAE29097D509862D23D7A686A00A9E2D546E7FB20CB598D1B97484A9F C674B7E04D76D9B5604BE8EC843DA376CCD38C2C2567CFD80740D6A5F55FFDD9
23	V	E146CCA1EFF2F04EC445410B184FFD789FB6D9C6EE95023002CF7A3F03087519 3FDCB48F5B95B95ED8E91F9E6A46A81FDB8C161A241FEF53378A04191B6D7B39
24	reseed_counter	2

5.2.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	E142209AFD9E77D264030161D7EF1C423DF7DD444B9A770F5B9629AD
7	V	EBAFC5112C43CCA72D92C8060AC5745524EE2846A1E759D2A98E3EBF
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	77B6027B93624B01B35CA38A031AA3C33A6C24443F41174A155806D6
11	V	B5BCF4AA3CCE4FA65442FD02711D81B77A20993E8E4E57E1DB90F11E
12	output1	561C52057579057777FB0FB06B3E222008876800076DCA67607AAD2B82CB17D5E 8791BFA293884FF52D6ADF94D91AC901A7E1F32769D6B1C9
13	Key	31F3F7F5FB5621A70BE8A8B5792C458575E45129697E7A23A6534C68
14	V	CADC8DA4721058AD28B01591DF7610DEEFB51BE48B8EAEA956AD2D1B
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
18	Key	51B50670F26BDC12BD608FB483C32AEF26DE0D1AE8AAADC861508594
19	V	E5BDF94265571B07CC8A5E5ADA71740C762E1E9BD61ABE084AF3DEA3
20	reseed_counter	1

21	output2	645CD883BBC129A75DC8289DB0D5662B9A8E551635151F70EA8BC25498D39E29 801823591ACF1309D3192A5095A92C9C1DCD40FE4E353F78
22	Key	DA8F25F10C6739E0A459229717DA0A25D11F1E7199BBF256610468BE
23	V	5F5DD9CA6A4DC5DD0925FC06F2251A4B9347CD0ED9D89650853B7742
24	reseed_counter	2

5.2.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	D8EF3FFDAF4157DBBCD84380AA38A9D30F7C4818F0E9D6100E2107F5D870FDB5
7	V	B4F20FD25FE1966D249472E51927624EDFC76548A61A75E77A1741EC65E040A5
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	D50B395FD08F5BF7A333CAF7D93523145FAA12BE8FDA6249505BEE86A7584271
11	V	EE27526265A03B1A6363F29C1DEC32D113A7C4EBEA4BD77B4F65C9B4BED56154
12	output1	929126C5B0A16C696C509E38A1135D462C74819836741FECA184CD94A6928A63 D190C28B75264202986FE51A1EAADBE56C11435E4E6CB9279AF9E052A345AF1F
13	Key	9879E07298272C722027EC4BA9E11E2667569008A8F01AE4F810AC2380564C7C
14	V	A3CF592B62DED4F4D5B776F604B2A112745EDB892A88204382E6F3C841BB8FA9
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
18	Key	38BE3F366C2F726FEC94B8EB3B0F5D1B38C32FFA483E9FBEB0C15DA2787D2C48
19	V	5A7421C03E3413A1B0B915A39D4927F7B61CFB06EFF63746212A5900C9C3F95E
20	reseed_counter	1
21	output2	2E914322B3853024039A8A93BF831B8CA33909E3F162B2857B26B52D58CD8C14 294E958BB1B6C5F3C511EDE2511F9CC2F31EF528543A00901BF9006E79CE4F72
22	Key	CF9BD44C98D1A8E054BF52D7E08DB8E586A1F6F468E3A6E4CFFCE03D4C049C04
23	V	9B6D4747F33761015FCD1891399F3252FC186A3464DB5CECC51238CAC869812E
24	reseed_counter	2

5.3 시나리오 1-2 (개별화 문자열 미사용, 추가 입력 사용)

아래에서는 시나리오 1에서 개별화 문자열은 사용하지 않고 추가 입력은 사용하는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

5.3.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	55B1F0D6AA834CC67177CE81CBD81AD8A62E7A60CFB317FBFCA650DE4E3AD420 36A33E24FAF77D4D3AA9698C2FC2015C300ACD410140E5D8
	output2	4A00486F4F60223E1E93486A8660B47F682BFB06F1ED97131F7577F60D69EE8A 951DFB4E356EA0D5FBCCD0F4E3CB41457588585459B6921B

5.3.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	4DD3E05CE9B759B241295144CA56CF41280DCD5A980BEC2FBA32F4E6DD21467F BA2506531E9449AD2785A249D333C73EDE146B1AE015F0A002F3A27F840747AC
	output2	64459E9BEA1C07D4CAB4F4BFABC90D5ADE60D56DED68818BB203577A278DC0AE 45E086B3447FEEA7420CB3EF85E303E037642E242696B5B5308C22FCF046E83A

5.3.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	7DD1069908B372BD28C04A0147DC28DC837D6CB80CDD42227100370DEAF1391A 237C2E322E687F684494BC6CA72D309E0D7C36540A1654D3B82882D5020FB891 AE3A0AF417BEF1CFDA366E1579B2B970C92B26818443BA8C5A704164F73F8203
	output2	3BAD8AF540C6577D930C1089DFFC626725149AE7C1D2E3A7299E51FC72D7FFD8 793E8101EF1D77DA91C2FE961E4EF021E65FB91E416764585C33143ED0BA54BB C78FD9A946C723DA4DC7E0E4AEF354ED6A4EBCD3011B0F0FBB7AA42FB1C0B982

5.3.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	494A234379F22E961E9D2DEC8BDB4E674B3142C57189807B49FA254A027081C1 92EF52FD1BAA23515A2CDB58C142F4EEE3D61182DEE01106296348221033 31FF 2E91BA81A7F0873B16BAB1F727B770B7B3DD4D5AF0FA5A3C76AD4AB9B04B88C5 A4D852FF54048592EE5B0CBCECF17CC1A777F10B88D07DC20F3F5F4E8B15AE1C
	output2	4BEBA970715190D28EA9ECA7BCAD86FE56CCCF6E7FA7C838A16065168CF9DFD6 9BEA80EA17B4AE18DC7EB13E582C8E628A92AD3E9ADBB8BB0190F0ACEDE6C613 890A5C9AED271DCFC3C1F4CB439E5A4BDE5E89B7EF3B119EBDFDD49B0AE592EE 3B079DEEFB4D5AD339C032C842361C89808DC1147465D7CDD4294CFC5B4F9EF7

5.3.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	321B3E46D9E4AED0FEFB1953F60869E2DFED9A44AEE31730DD46FCC81310AC705DA149F4526E442A60DF5F4BAA5F18441CFFAAFEBE7D882D
	output2	869FBAF17D10C755A7AE0D77DF4E9186F514BEFFF7060CA932D6776258FE9AD1573770C61D288BBE976056227DB6EE371872170D53A21CA2

5.3.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	82DCC4EE6E866ACD8F1F17C446E2DCFE58DC74A0DCA09656C3C4F23EE6F6272C4FF07B4C6997329366658BCEB5B347B275DE1DF5E681762290B169CD1BD9CE52E
	output2	0F388F2082AE382D747C7E7D89C8139A0D7FB37A985D28F190AAB9FE62C1193DE4CBCF5C8301F1E5C4E659D6F51814D62F455ACEECAA99AA49348F81094C7DC3

5.4 시나리오 1-3 (개별화 문자열 사용, 추가 입력 미사용)

아래에서는 시나리오 1에서 개별화 문자열은 사용하고 추가 입력은 사용하지 않는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

5.4.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	6D899CA1D174AA6907235427CEACE651027A578EF8D35CE0890DEC6E94D8EB5D 9B5E61867261388C8D3E8BA0F679F5C99446986539166F7
	output2	CD3D36510489276858E02B40EB4EA2230272AC0713E309279752ECF9B36CBC68 BAF4A29061F1340D7EE9B4D62F05BC3188BBEAC659452186

5.4.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	DCF193213AE74C3703DD4141A5CEC182D8A5A2B7B1EF64926216B3DE8B8A807A 76C3152522225897457612F97EE7241E066BF49790CFD82CB1265137F03C9348
	output2	8E54D26A3F3B7097902268D667D19E78D7FEA74F80AE6D23E7806B412AA218D6 36057FFE4EA8F0B9D0B235335480CB060F583331F3053B96288BFAE9D4181B96

5.4.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8A5979D58D90A23CFC38D346A68437B973580F5217799BA68B87FA3CC1C23584 66DF667036D8ABD79C09C80F2CDF8C7263D081F478121D8898A7C46AFAF27A65 00105E3A633BE1E95BBAFD1F98C834A54E78B3D3CE341A78A926EDC3B4648D7F
	output2	673BCFEFC6368755467E47ADF964D4B45DDEBB0125486BC73767F192CE60F09E B7FA778A08569153852C5AD34957A18F6546F812471DA106AB7A2772844B93CF 6BB4E8C7A951B168EBBDBB08748BE8439EC8C6F830CD5B9D52993E8BB29FED3E

5.4.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	96837248B109476B543AEAEC2F081C8742BD61E30E7034D2BFE4C4BA1061840F 6086EAB302AE262E90BA6E000DD19BD268288C56F34E8F91F5A53C15DCA215FF 2CE2B35B713620634B42723DB3DA911542694E24B5E09F0F05E882738401A9E1 672882EC1068419EDF209CD34FB562567385A652C1E20E15BE9CE6FC4B8007EF
	output2	C6E75EF94D676D09B2C82A1EEB81126AA0A4A997435CD6691C9C776AA64A5022 64F345B8F80C4B9CB0E43743AFA3ADC78012CD435438D68909BA8282CB0F4B87 AC1C33F2398BA9AE328043EDA7F661B89AE4807611BEEAA7B73DE43EA789AE4A 031A3D3A211FABD8D9AD4D8197763EF5649C8AA3CAF82C5127FEE59EFADD1976

5.4.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	0613457A2E9EBB4A51274410E379B238C55718573D7843B1BC4BF6BC0825F442 B21A108443B5B253A21B599BE32DDAB2EB350F7371133955
	output2	E1710AE49B1C8F02F947CF0FE199B3E9F1423CE29A99CAF5B0182FF99DB2CC8C 9946393F887CBABA4D9098BE4E131A61E9362C9FDFA83423

5.4.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	CF452A3E17FFBC0890B2914756ED338C1E600748E76D71CD94CD0573D57239F0 AC5145C94A17B8DE5E4173B400D3622985D21381D730E201CC7FA2443622F182
	output2	852B3CE525D7B56DC146673127FA77D12D47AD26B65F8CF3D8FD1FB88D99F3BE 5BAF4ECEEA8317FC5BBFA235039422580EDF11D9B031D510C9C7F1986DD8EF01

5.5 시나리오 1-4 (개별화 문자열 미사용, 추가 입력 미사용)

아래에서는 시나리오 1에서 개별화 문자열과 추가 입력을 모두 사용하지 않는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

5.5.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	A0E5E3DC40F0AF78F5F8334C8818BEF89601DF1A06FB5F648A539B93369F3169 866504551CF35860B5AF5173E1FE71091AA4D1AD4987AB83
	output2	C4E1FAF34FF1A70FC2C04CB1CA4F03D2F502E7C4416761A83AA84153FA15D085 6B0EFDDBF0081BFDF4706BE8243D54A0C9CEA1706E0FC025

5.5.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	4C645CFB4D4BB1E92747E99F30EE7447AF5B4FDC4658DDCE781E3EA816CF7375 B9EC097A0FC3DF5369A2665173B191ED3CE69634CEE615958538C34CA7112FA2
	output2	8135F97E06D043CD67EF0B631AC8CE67F8867DA128AC3D272C2F6C797DDB8B87 999D7CC2ADF17A507658E834653BEAEFD663D6E7118A97D333197508D5309414

5.5.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	AFDE87B6CE4710BD45630869289D5EC3BE244AC6ED2BCE7A5E47D9D8A286B69A A84356E38D424962A8F257FDBF35282CFF1A3A9A5DBBE39466FF5AC8C48B56F1 2A54EF1988DDA55BD0EF7C1C11DEE90844EF2A0DE9F3B4F1674A015A0F75B11F
	output2	0B7F42C927A42B919C36942FF87519C55506935739447 02E8D415DD0AE2FCC3B 34F3515FFDD7F72B408EB1E38B027930FE247C6B57D536CC4B865D2E47443073 284AB4B907DE5663533B73297B8C93591251372B41FFD71B2E3CBAE785CB40ED

5.5.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	D4A4C5A32A97BD892E05B68138F4663C17C1672C0C7C42A6CB8B37862A107737 C36FE32568D00C478FD8C51695471F317621A3330C1F162407668AF5D7C547C7 BCD58BBC3BF5A07ABA3476EF1823EC77499F17337CDC5C763AAFC035CC4CD9F7 B2975173906D00BAA7D81B6424DFC2F59D503A960A4F5FE3D9BBA91DAA52E883
	output2	1500E28E81A34B91CC1B1253B1593A938207F454F6F95AB59828579F4985304C 747CB10DD2EFBFEBD710C8E2B5277801FD863A253B43A08CF110199721FAD6F0 75B2CDC2DE36C4DB3124DF709A97451DA346362DCA0880E7A2BB685847909DEE E168D448493985971 36E08ADB8514F59EAA688FEB26E915FBA447B104506F2EB

5.5.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	37B59423C0B24C9A13ABF715C870139A5D71972A1B8212D0666AE883314CD69B 3208F6A6451DEDA1390C00B7569F1115E0A4E6D00852253C
	output2	CE339FC9B7F8BE71C73DF904DF0A4607298E57689DE3A2A9F80AE93163CE17E1 EB5E487CA98A4CB2B1E0C6B167A32D6951D423A30BB19EA4

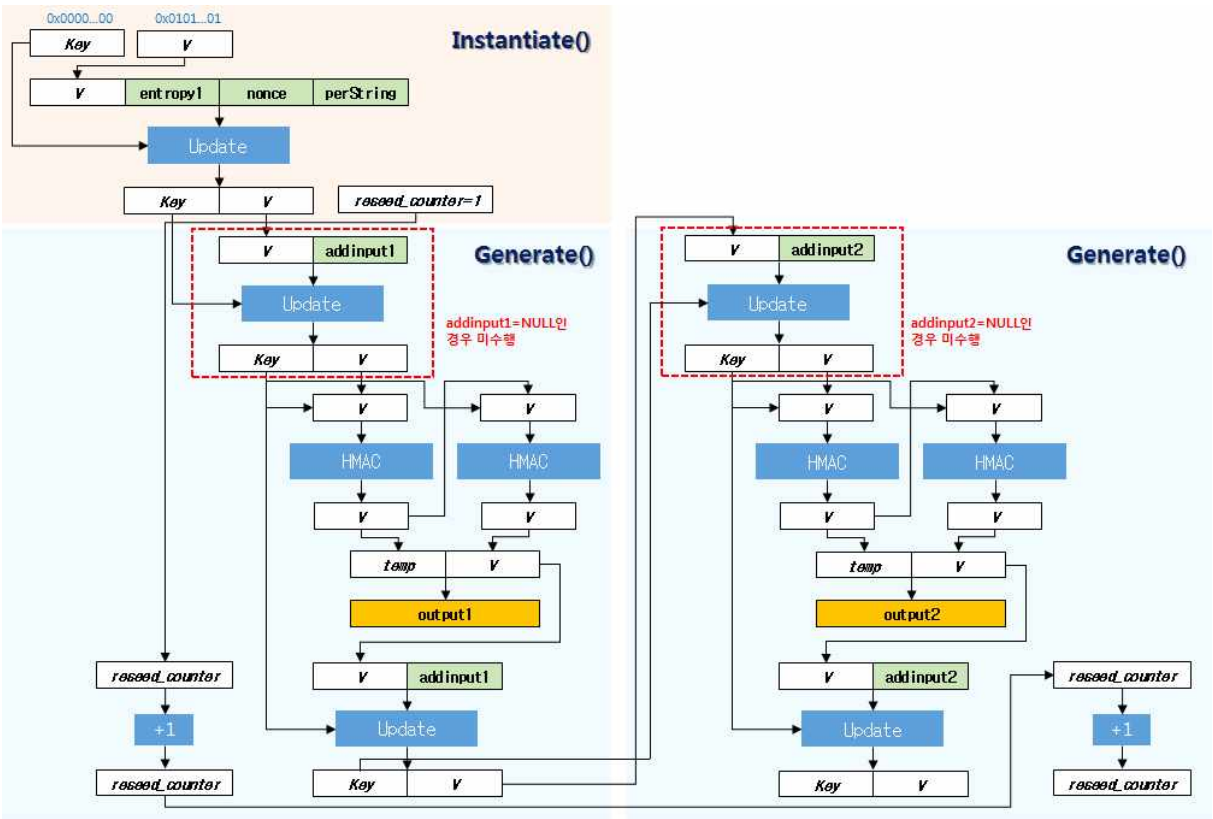
5.5.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8355C654CCA07D303919842C240ACCAF9200C3FBA42C88C1C565FA23A02382F1 43172FCC57A0FA4A4EACE0B6D3E28F517DC5AB59A6CB0E7359FAB6FE74DD40AB
	output2	9216D9DEFFEEF5E7AC856BE8FD8A3BA2549DDE6034E784729FF25BEF866C2DCE 24C2FE1395A923C3CA2EE999EEC5226A6CC30851AD345E3DABE141D8124CD791

6 시나리오 2 (예측내성을 지원하지 않고 갱신주기를 2로 설정)

6.1 개요

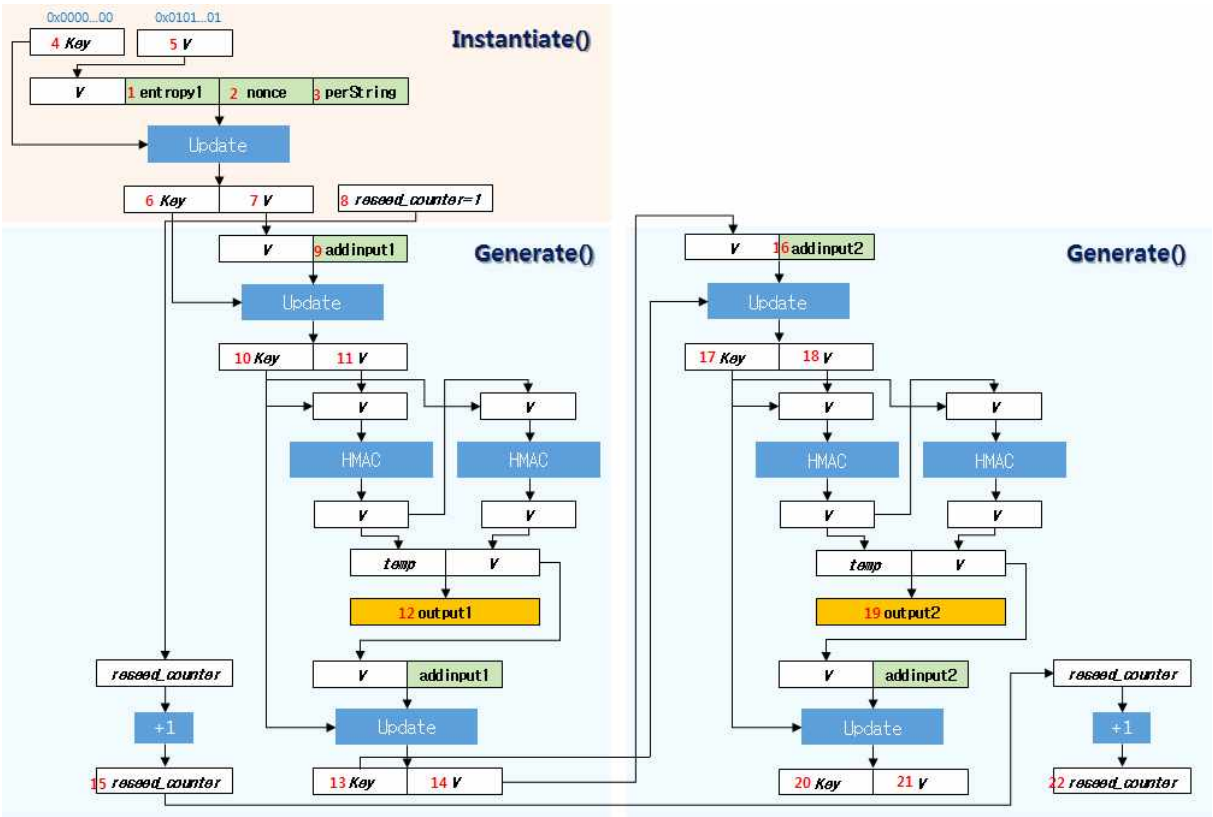
시나리오 2는 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 2로 설정할 경우의 HMAC_DRBG 참조 구현값을 제시한다. (그림 6-1)은 시나리오 2에 따른 HMAC_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 6-1) 예측내성을 지원하지 않고 갱신주기가 2인 HMAC_DRBG 출력값 생성 과정

6.2 시나리오 2-1 (개별화 문자열 사용, 추가 입력 사용)

(그림 6-1)을 기준으로 참조 구현값 확인 위치를 도시하면 (그림 6-2)와 같다. 아래에서는 시나리오 2에서 개별화 문자열과 추가 입력을 모두 사용하는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.



(그림 6-2) 단계별 참조 구현값 위치

6.2.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	5527329894A1D3205839AA918031934AB3BB24E382B828E334789140
7	V	CF1F4580A206D2222974871186D8D2E3CCD6F3E04EE8B54948E4E754
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951

10	Key	6420C403615EF44A796D0F9F856B4A30E7E8754D0ECC48723B44F059
11	V	EEF8C4B33C85507F64A6A21611CAD58F7BF26A4E2C68387425563 98E
12	output1	FEC95AAA45FF9D23093B44B6C7A104EC6E85ED7AD5C6650D1CDAD05F6EB8AF20 2F0D680B33D1C3E95AA1A9AD79BC343D47F24BDFBAD2EFC2
13	Key	61E711ED2E5AE44F1928F52F600418D274AF871B35192B0B2E4657B3
14	V	9247809F696656459F42770264FBF9D16AFEA9438C818C999E6FF54D
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	1046F464757ABAB866E0C9340BD05E0D2F0E13A9465E5F1AF9E3D589
18	V	F125054FDB3D4ECB436EE4E880300634BA6D80275120 89C1952B5077
19	output2	46322592D58FD4744A017D3B73BCC02A82461C7E7C23EB417BAFF168B4E06293 722C8A5F3FAD317D4B1B15D371C3EBD35FDCEB5D11571B93
20	Key	876A829F54E15FA2860539E3C5A5F1B24ED9283920B29F823A20B5D4
21	V	B7D085611EA46870ED409F8412E22ECF5FE8ECEC23ACC17A112C1AA8
22	reseed_counter	3

6.2.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	2FAD2936439B2CAED4A7C2831922BD532B43319DC8710E486A005B438F92B692
7	V	D9197497970B52B4B40FA99F208A5F2C5ADBC1056770144A29E8708C0474BDE2
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	1FD227D76FDBAC223F457C5436C0B12E8672BF5BFACEF680CAA577D036D06695
11	V	FC1091CABBFC11E90A795AB6324708C698CC8A81037442AB62E66089CDB9EACE
12	output1	1A679AB4513DEBB0BACD81F3E771727956DD4C8BABA15D8F1E197AE5DE4B85C8 2F6B01727B494F343DA06A6C5CBBB85D32C4DBC5D5AA64CAEDAD6A417D4AB0DD
13	Key	90D15019B8B9E9A3BEC53285ED757D0675902CC9D84598C1AB872AF8FCBF0EE9

14	V	98F0F75BEE8285D6ACFFB93AE26DF8F6303BA687A0D95F04A2EA0CF62606C334
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	99720A6712C34CA691EDD19C66FEC1EC219B5A6CD3F3F5A35FFA06B5C3D46833
18	V	7DCDFE4E2DE6C6FEBC3059627D16AC465919AEC8C94FFC70E51501AAB3AD3884
19	output2	D28B2E9A50A54890F8BC61959D7EF5F39DFC0A5B31955A46FCFA73D9647D7500 8C592843258D5F7FC81BFAFC0882ED135A929B1488F7696FFD896CD80D44A2CE
20	Key	E4FF2C18BEB554663A2C55FE73075C50D4CB3C43786EAB5FE461FA80772D8501
21	V	7DB9D1C72D893A10189DECFBE428998FA00D2AFD282A46AC88CA33DBA04D1E7A
22	reseed_counter	3

6.2.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101 0101010101010101010101010101010101
6	Key	29CC03EF83F7577AE3C69F455776A27A6173CAB7E04412E8684367D52DC500A9 497ED86EE319700FDBEA3E87A7D6FD51
7	V	2D0CB4A09EAB51CB8A3177B0AF2F386B685306A21591F3E2C532FC9066857A72 19277BBD9C76CB315B78F76511325731
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	13AF35BE8E27D3BCC7212BB59BC4F3A87FBC7EF582E7D3E76B31CFE1258F70DD 2E7EB3F7F7FD2510449CCE6B3D993A82
11	V	42EA9E4E5604F8133A0BB1330F1A9F0AB714FEADC31B9EF50EB6DDF5E2597A74 63A7C0C92EAF6B7DE679AF6F90040827
12	output1	DFADB57F484AAE379BAA9E362285E955DD67C55EAF3ED1D485AB6789B528869B 3C17D6257A876E45DE80804620291DCF95AAD6DCCD5BEA1CC622C4D0589A5AD2 F986BC1825D6BDA70A84ADF17CB51321873E8BC19D0668757C4A12B33C4792EA
13	Key	B326B85DEA0E975F21B41ECC96AFDEE0C9575F8AFA27E15918FB65C2C184FDE5

		607CA1CD93A4BE066D379BD05A312C67
14	V	7C359E33A4A899D4D9B19D15ECA2B09FB2FBF3687AB449C697D581446559B23C640C3AAE986182A977B83225F25BE2E9
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	53EDBA2DAA58827DF8445546B616D560BD584F27EEFD1FB2A7F4DA81471B16CD45C2FEA13B1F353B938E61537269AB60
18	V	33F4967D5C46E218F8F7CCBC0CC2DC739967CA0BE2DC0B934379AE94E78D6D27E289D1A02291FE4C4CC9065311C420C4
19	output2	506F2DFF37935E31191CE2F67AC55481A46C03E20979974C2E90DA54C18FFFA3A48B6C6F3528D123D078FAF06B59413EA4FAEA79424E0B2113493E6DC7DB91AEAF2A35DBA58D222FADEB96A64E78A1505D85F08B0914D972A8E0FF0F10C869AC
20	Key	BABADD1D028F8AC002B0E1FB8AF645F164928AC21C42B81BECECEA385072534A8B98C04884CE02266CB2859E421B9913
21	V	15538759BE1AFF4C6869492805059000FAF518B3104E9FFFC78413EE8FD76896F11B5C0846192A33E1D4B07D1ACD8944
22	reseed_counter	3

6.2.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
6	Key	03CEEDF46432B9FAB1D8400BE97AFB38A8118B793EB9ECC00F3BE53163741EE5B0EE7B5327697E26E0EE8D426AA1A8DB373F4A1D1B8402A141AF5C18685431EB
7	V	6BEF9B37F8265CCEF1B84CFB21284B8ECD9F4166B2FCB3E93B3A262BD9D0788D5A4B236E808E125C5880591D545A73CBFCD9050C7E080789BEA38AD5F4C11432
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	BD109D3AF433D79016125D0431DFBC1EF610284FE8B963E7FF0D82EF0B0F4B8224CC9599E15DDB04626A88797468937BAD603A6E33CDEFB95B1DDA5A6C111B6C

11	V	EAEB8EEC0F52DD57B2F48E2681AA182F4EFAE65EB28BD782DA1FA8AF1590BFCE 2E44861F82ECBEE1687C0F7740B301E0B250F386F6A05CB2C77B9F02FBCDA0CF
12	output1	4079EC4371DBB9635FCD8FE19D265811E0BC885B49570769F673D0487A6D2FC4 3C66F01974B90FE280C8293492 58C1B78A13BB134F426C45AB01A12AC96EE609 B7189A13CC2949917D31F95590E6856ACEB3DCE5C03586F5F75676C6C14E221E 4FC68F4A55331613FDAD5ABC85F12C4D25F92D69FCA446F6C7C9C44CAFBA997E
13	Key	338F51647751EEC121C6D61AFD4741632DAA1BC44EF780753AB6C844B808E73A 0016BCE6919B0775376236BFE70EF863A9557FBB52A18DB298BC4ACF4556317A
14	V	F34D765D27C977A697819F7D4DBA9833D060660898C86C3E2F229FBEC54FBD94 A82007B0D03D4A4B60D9CC7A6C62E17A91C65C06A16FC5F443D2FC66C3E9915C
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	F1D4BFAA6AD322DF8FA322D270C3E3E87CC2AB8FFC80641C58CED2699002288A 659E9BAD66A7AE4DA2BB584F4461EA9E0E8B62D24319258C38ED7219539B85CA
18	V	E13A3FE61D43CD2B6098FA28E70881996042AFC9FCB2FF469D980B9A17530FF0 31400384ECE66075E6B9FA16A68FE111666D3783DAC5E69806FE31202710EC20
19	output2	4DA69331BE4572061687 1442C922300F8AC33F5B2EEB6B433AAB8110BD428703 00434CD0DB07BB664CBB0A92F12980C5E7FD6D90FD636B85DE1E8AE0663C6C6D E0DE2B2B2050383D4DDEF228CAA637830349B4EC8A5B6173455E17F7B60D210D 7A575934D307056E9B874D88F1FD81B7F6AC1DDAF4FB547E0C54CF2E384662D1
20	Key	3EF66B9F81DF481A0F3CCFB58BAA03519355FEA5459C6ABA2BB2E373BF586787 E61E240866221D820026CDAA182FEA0016B6311E057664D267E8346D2E7B00AA
21	V	C10076C7F8DEB5A66B4BB2CB07FE0C44B33A06678C64FC818DCCD8C9D7EE9662 F64AAADD717DACD7C7460BBFABD84BD3D22B62333A9A6A4B86139D96B9BBF179
22	reseed_counter	3

6.2.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	E142209AFD9E77D264030161D7EF1C423DF7DD444B9A770F5B9629AD
7	V	EBAFC5112C43CCA72D92C8060AC5745524EE2846A1E759D2A98E3EBF

8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	77B6027B93624B01B35CA38A031AA3C33A6C24443F41174A155806D6
11	V	B5BCF4AA3CCE4FA65442FD02711D81B77A20993E8E4E57E1DB90F11E
12	output1	561C52057579057777FB0FB06B3E222008876800076DCA67607AAD2B82CB17D5E8791BFA293884FF52D6ADF94D91AC901A7E1F32769D6B1C9
13	Key	31F3F7F5FB5621A70BE8A8B5792C458575E45129697E7A23A6534C68
14	V	CADC8DA4721058AD28B01591DF7610DEEFB51BE48B8EAEA956AD2D1B
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	47B8B65DB3DA312ECAB28A86F22DAE48231663B46A4D56CB66D9005A
18	V	2271F2123E31824706716F6374C6DE66C085472953561CF152F00CF5
19	output2	3260F724A2D7FB3689CFE3898855F3AA7AB2376A74E957A71DBE184E45E87DF6BD7466C88563E020DDC5832D2D8D35D90EBB007A33D2F9DE
20	Key	82E6CF5BBD33AFBBAEDDE04BAA886812B8F2F515FC09FE53A3A4AF5E
21	V	55F3C811B80F64614EFD0C20D3E80A78EBF3075B9C7924D11AC0F6E5
22	reseed_counter	3

6.2.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	D8EF3FFDAF4157DBBCD84380AA38A9D30F7C4818F0E9D6100E2107F5D870FDB5
7	V	B4F20FD25FE1966D249472E51927624EDFC76548A61A75E77A1741EC65E040A5
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	D50B395FD08F5BF7A333CAF7D93523145FAA12BE8FDA6249505BEE86A7584271
11	V	EE27526265A03B1A6363F29C1DEC32D113A7C4EBEA4BD77B4F65C9B4BED56154
12	output1	929126C5B0A16C696C509E38A1135D462C74819836741FECA184CD94A6928A63

		D190C28B75264202986FE51A1EAADBE56C11435E4E6CB9279AF9E052A345AF1F
13	Key	9879E07298272C722027EC4BA9E11E2667569008A8F01AE4F810AC2380564C7C
14	V	A3CF592B62DED4F4D5B776F604B2A112745EDB892A88204382E6F3C841BB8FA9
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	68D2046B6CCD9B6E611198FE3157EAD07968ACA179AB1AF57538E89B69AFE3C5
18	V	C5ECE7A042CD61E20AFD3A0C955EC1E9C00C2AA257C6FAE35602F7872F3F3E1B
19	output2	702B0FC5F022AAFE6AAA507BEE421FE52ED6D00560DC87A019AE89AC4A761A04 68EBD5791FAB81F771100E8D399918F048BE11FE63F9D59F3F344575D35EBA75
20	Key	D07A9F700AFE908EFF4161A499E82B80403476E0CB1EFE587BDC7D4A4F2B5DF4
21	V	76AA21EE71E5CA636B693B07D439270C1DD1F23CFA19D438F86720014023EA92
22	reseed_counter	3

6.3 시나리오 2-2 (개별화 문자열 미사용, 추가 입력 사용)

아래에서는 시나리오 2에서 개별화 문자열은 사용하지 않고 추가 입력은 사용하는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

6.3.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	55B1F0D6AA834CC67177CE81CBD81AD8A62E7A60CFB317FBFCA650DE4E3AD420 36A33E24FAF77D4D3AA9698C2FC2015C300ACD410140E5D8
	output2	1B47A9424C986315EA99713822F2DF998244DE7B2AB51667AC2F288C1B929826 E181E85216227AC78F2E60355BAC29DABA5FAA04222F0C3B

6.3.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	4DD3E05CE9B759B241295144CA56CF41280DCD5A980BEC2FBA32F4E6DD21467F BA2506531E9449AD2785A249D333C73EDE146B1AE015F0A002F3A27F840747AC
	output2	8A0DFCAD4AB492ECA76150FFB4451FBB90245AF8D184D25D8D06A1473E6A34E0 7386259FA915C3C8223F2F3CB9AAAC2D60A55324EFCB6D71DD239DD9525DD8F0

6.3.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	7DD1069908B372BD28C04A0147DC28DC837D6CB80CDD42227100370DEAF1391A 237C2E322E687F684494BC6CA72D309E0D7C36540A1654D3B82882D5020FB891 AE3A0AF417BEF1CFDA366E1579B2B970C92B26818443BA8C5A704164F73F8203
	output2	D3E7E86CA17F6B4C1BD9A807A8EA89A47274CB79AACB52182BDE9F1D681F9244 2665F11FCB9877AF6C51FA6FAE65D9C433F4D3B5FA6219BBEE18D140AB118FC3 9B1F541CB79F56319A60C9F2E838DC928BD45732F862B555B9D23BF86FD35285

6.3.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	494A234379F22E961E9D2DEC8BDB4E674B3142C57189807B49FA254A027081C1 92EF52FD1BAA23515A2CDB58C142F4EEE3D61182DEE011062963482210333 1FF 2E91BA81A7F0873B16BAB1F727B770B7B3DD4D5AF0FA5A3C76AD4AB9B04B88C5 A4D852FF54048592EE5B0CBCECF17CC1A777F10B88D07DC20F3F5F4E8B15AE1C
	output2	17CF2DB62B595F93F1DEEB1A47443D972175A77AC08FAB0A22BB679F7BF20E73 3FDC303327EE8893F138D2A97E764F4F69AD8FF4502A1D0429F7786528455CA1 24CE5628B399462EBBB03E333BE3C9FAF88710A7939E177073860310B4B7168C D0270204A825E956D514DCEF19E840D03E64312F6B6F9E285C220EE66C61F16B

6.3.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	321B3E46D9E4AED0FEFB1953F60869E2DFED9A44AEE31730DD46FCC81310AC705DA149F4526E442A60DF5F4BAA5F18441CFFAAFEBE7D882D
	output2	673981E6A006639933BFAB1DD101631A36272A8B4C127CE0450135E860D4CBACF737467882EDA1B30F95957CE1495BFB613AAC510BC59908

6.3.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	82DCC4EE6E866ACD8F1F17C446E2DCFE58DC74A0DCA09656C3C4F23EE6F6272C4FF07B4C699732936658BCEB5B347B275DE1DF5E681762290B169CD1BD9CE52E
	output2	E0A5A1D9441A41A2073D58544A73214E3FC90ED557FD4490EF154025A9D769EDB16A9F8F68F9649F0AEB34CD777B8CE3CD6ABD12464B9A72132FFC654E992A06

6.4 시나리오 2-3 (개별화 문자열 사용, 추가 입력 미사용)

아래에서는 시나리오 2에서 개별화 문자열은 사용하고 추가 입력은 사용하지 않는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

6.4.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	6D899CA1D174AA6907235427CEACE651027A578EF8D35CE0890DEC6E94D8EB5D 9B5E61867261388C8D3E8BA0F679F5C99446986539166F7
	output2	E2BDA8C32E8065DBC55F3C07C6617DD68B99B0147707138B309D5CC1F8022880 53A575B098F9105853133C60EEF805D30A4F1AF3978C210D

6.4.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	DCF193213AE74C3703DD4141A5CEC182D8A5A2B7B1EF64926216B3DE8B8A807A 76C3152522225897457612F97EE7241E066BF49790CFD82CB1265137F03C9348
	output2	CDE61AD8B4B92FDF093A4B8FDAA95663D9FB2B37898140B0AF6478A33CDEE16D 931317A68633EB8BB8B0C916B087AC7610850A91AD0A2D5783BF7B60FBD57242

6.4.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8A5979D58D90A23CFC38D346A68437B973580F5217799BA68B87FA3CC1C23584 66DF667036D8ABD79C09C80F2CDF8C7263D081F478121D8898A7C46AFAF27A65 00105E3A633BE1E95BBAFD1F98C834A54E78B3D3CE341A78A926EDC3B4648D7F
	output2	15DC806550BC0EFBD1B3D90397881CB437B22910B1FA90D59EE7E1328E176CDD 0785A9CAF01E08B7C9BB58D0C23F1047173D0082FA73E5160C33916CFC2ED634 7DF225CA6A41061D1E3FCBD8772CB4AD40C22F4B6736E3FF9A0630B237E0AA50

6.4.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	96837248B109476B543AEAEC2F081C8742BD61E30E7034D2BFE4C4BA1061840F 6086EAB302AE262E90BA6E000DD19BD268288C56F34E8F91F5A53C15DCA215FF 2CE2B35B713620634B42723DB3DA911542694E24B5E09F0F05E882738401A9E1 672882EC1068419EDF209CD34FB562567385A652C1E20E15BE9CE6FC4B8007EF
	output2	2DF75F53BCCAF27964B735BA953764D6630EA88F892456E46A6EA82BA120A180 4EBE1760F4E9672F5187AD0EE82F8EEEA878B0A2E9148049D2B60CDC5106E477 09F28734E8B4784E348F8926419B6339F38DDDEE615AFDA2F2C2597CEA24FA39 05BCF5F679B0DBF3993C3E0634B0FC8A9059398F8521A34C77B85389971B8F32

6.4.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	0613457A2E9EBB4A51274410E379B238C55718573D7843B1BC4BF6BC0825F442 B21A108443B5B253A21B599BE32DDAB2EB350F7371133955
	output2	0B348F3495B3857599CAFD0AE0E0EE960916996939A82314B3A815DA2979C2AE 5E3BAABB1C9DFE4D82B46D94573F451BEBAA96DBBAA8F6F6

6.4.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	CF452A3E17FFBC0890B2914756ED338C1E600748E76D71CD94CD0573D57239F0 AC5145C94A17B8DE5E4173B400D3622985D21381D730E201CC7FA2443622F182
	output2	95BA3D597DD2FC11743B47AE3CFB120B5534962BC22FF753D31472B5FE506A1E 810DDEBA76E862FDE38F68B88B49338A95880C969B7313FBACBD0F62A0EAF1B2

6.5 시나리오 2-4 (개별화 문자열 미사용, 추가 입력 미사용)

아래에서는 시나리오 2에서 개별화 문자열과 추가 입력을 모두 사용하지 않는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

6.5.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	A0E5E3DC40F0AF78F5F8334C8818BEF89601DF1A06FB5F648A539B93369F3169 866504551CF35860B5AF5173E1FE71091AA4D1AD4987AB83
	output2	D911F0EFEBE21EB7A76A8C302351384691 9F5E80B8019CC291A240F544B4A21E E1A5E0ABB6A1EB7504891936E192AB42569F8CBAD8EB45C7

6.5.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	4C645CFB4D4BB1E92747E99F30EE7447AF5B4FDC4658DDCE781E3EA816CF7375 B9EC097A0FC3DF5369A2665173B191ED3CE69634CEE615958538C34CA7112FA2
	output2	93257752EBD6318008EF176D48DB4AFAE65DE65E0AD5492AA8A46B69E042E724 8A7EF3EF4C1F7CFB632D79B459E2AB2F2215B30D64E79982FBFBDE07AD5596FC

6.5.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	AFDE87B6CE4710BD45630869289D5EC3BE244AC6ED2BCE7A5E47D9D8A286B69A A84356E38D424962A8F257FDBF35282CFF1A3A9A5DBBE39466FF5AC8C48B56F1 2A54EF1988DDA55BD0EF7C1C11DEE90844EF2A0DE9F3B4F1674A015A0F75B11F
	output2	64C019EC7A327274F298474C2535305630601CDC7FCB1A50CB5C079F73F3C281 49384A7C1E2E73CC4C10A30C0B0244C148940300E4CD172BF247CA7C557431800 9FCDB09452B38D6E01DD6AF4FBD119C950098435338434B8B16C14080089B4FD

6.5.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	D4A4C5A32A97BD892E05B68138F4663C17C1672C0C7C42A6CB8B37862A107737 C36FE32568D00C478FD8C51695471F317621A3330C1F162407668AF5D7C547C7 BCD58BBC3BF5A07ABA3476EF1823EC77499F17337CDC5C763AAFC035CC4CD9F7 B2975173906D00BAA7D81B6424DFC2F59D503A960A4F5FE3D9BBA91DAA52E883
	output2	8064BC56A883F6BDBFC5E460B0691AD5B15AB7590521AD4DDFE8A677DDEEB16D B85A31FEC5803588BE1C77BF0B321B2FDC4E1D3F3F00AC1D6545CB64CEA99578 F1AEF35360B50AF276DBD937272DEA35F84C9A6F30D0366C176FDE74C014548A 9B3A1306A688FCE6F969388D0877B152B1DA85E80A202C3B4586534D3B355858

6.5.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	37B59423C0B24C9A13ABF715C870139A5D71972A1B8212D0666AE883314CD69B 3208F6A6451DEDA1390C00B7569F1115E0A4E6D00852253C
	output2	D462F7FAF53A76678B2487B7350E85C64E255BA156497D78ABD17F849CCE562F BC459B73010B11141125B084BF77AEEA7E2B11F9B326E53A

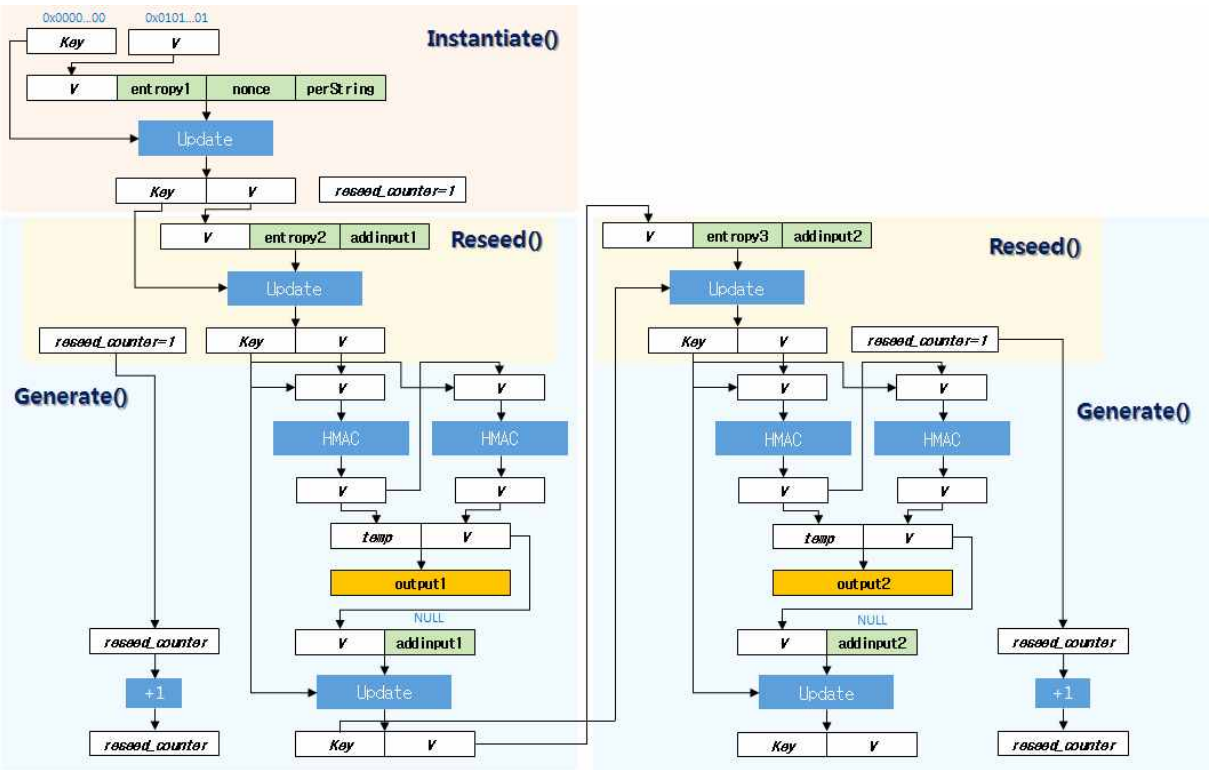
6.5.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8355C654CCA07D303919842C240ACCAF9200C3FBA42C88C1C565FA23A02382F1 43172FCC57A0FA4A4EACE0B6D3E28F517DC5AB59A6CB0E7359FAB6FE74DD40AB
	output2	71D7632A3321D43A35A948437188646F8136BAB62A51554C9DBA9B5EF044A161 AE6A2279A8D601F02FDC2DDE77341FD0634B9EE1B95A10655FF48B389DEAA981

7 시나리오 3 (예측내성 항상 지원)

7.1 개요

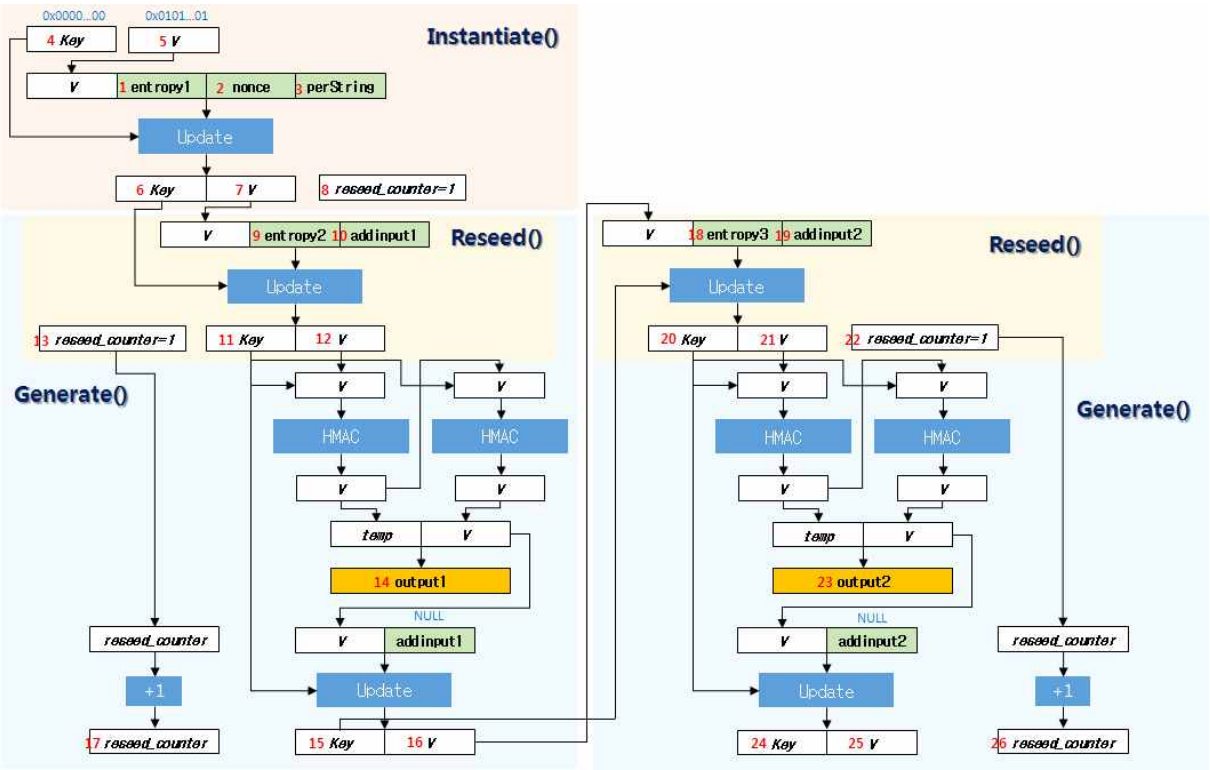
시나리오 3은 예측내성을 항상 지원하는 경우의 HMAC_DRBG 참조 구현값을 제시한다. (그림 7-1)은 시나리오 3에 따른 HMAC_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 7-1) 예측내성을 지원하는 HMAC_DRBG 난수생성 과정

7.2 시나리오 3-1 (개별화 문자열 사용, 추가 입력 사용)

(그림 7-1)을 기준으로 참조 구현값 확인 위치를 도시하면 (그림 7-2)와 같다. 아래에서는 시나리오 3에서 개별화 문자열과 추가 입력을 모두 사용하는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.



(그림 7-2) 단계별 참조 구현값 위치

7.2.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	5527329894A1D3205839AA918031934AB3BB24E382B828E334789140
7	V	CF1F4580A206D2222974871186D8D2E3CCD6F3E04EE8B54948E4E754
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951

11	Key	70DAAC36EE15EEA323A934177A0D845ACB8B631D902DE1F7C6720D72
12	V	E463F96A373255082775D270859751746BD44FEF8BDAB0E0CF0880E0
13	reseed_counter	1
14	output1	4987D2DC0FD9B68CEF2D3B05F067920F55730796B32E4864C8F9F41ECA5089DC 79C671113447B22D9F7D53E703EF7F872CA02EE03C694B01
15	Key	76F850AAB21C0F4C9A4F4D9238D26B0A7F6613D1C13D21F2EBB88C61
16	V	3F0FC9D87F17EC05D554F3D7286BE564E15A0956E99F0CFEE02531EA
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	4C07D751225E234309D37F504BBB249E69D3350B752E4EE1A23A5B9C
21	V	88A59B4CED0CEC203C93E9006B35F9BB3D2E57396BABCB83BB9A1BC1
22	reseed_counter	1
23	output2	206EB679C0DCE63A001347DCB5DA5886F3843884B3BE452C524D97C94BA1830D 8AD2A2BAC8B9D73B8E5619DCFE3A397060EB9E95C5C43307
24	Key	63E7974178EBB1E7813CB95F50D796A6C2A71EC4A0F17F910A120F4A
25	V	D33C98CBBE836041217682A3701F2B8E20DB67F626491B23D4C88E9C
26	reseed_counter	2

7.2.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	2FAD2936439B2CAED4A7C2831922BD532B43319DC8710E486A005B438F92B692
7	V	D9197497970B52B4B40FA99F208A5F2C5ADBC1056770144A29E8708C0474BDE2
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	2D90167CFA32AF5D4A86BB862765F0AE0B361BA8C28B45175831313FCBB27F83

12	V	218F524104ABD5EE41062A45686DBE99A7E56D860455DC8178113240A6DDDFC8
13	reseed_counter	1
14	output1	A8EB3DFB1220EB9E92402AB7ED0685C26A91FD3FA372605D05B16D1A53067CD2 04FD0DD43056E12B7AFD096F35085968069FA60E3395D6367419D9988FFF795B
15	Key	4D6AF24256C35092503F16BC3B06A1CABC8658D670DEDF736830542110FC3FA4
16	V	38B5A1A6A12615BC06A04CBF9FA8C75955148EC256A3EEBE0D2F3D00B2F3A416
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	817CC095C35EF92A7D59FE5EFBEE1B0C1F4BC4150006976696CA525FFC4346825
21	V	BA539DFFAE5289168057F81321796265A93D20801D0FAB6B3394DD905078F72A
22	reseed_counter	1
23	output2	6092C7C815D36C71DF9552859FAE4C74281B5A2DBB411E89D4B17D02F46840F1 1B0800CF5C1EB3968C93E9F274F08CB26C7440992BB372244FCF836EEA408C6F
24	Key	F6B24B320CC50EE96626A715392FEFA310A2116F13EF80CF02613D39540FAED6
25	V	708BCEB760ADAE21D8CB673273E8466B0D34584402BE25882F10BF5D52385737
26	reseed_counter	2

7.2.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101 0101010101010101010101010101010101
6	Key	29CC03EF83F7577AE3C69F455776A27A6173CAB7E04412E8684367D52DC500A9 497ED86EE319700FDBEA3E87A7D6FD51
7	V	2D0CB4A09EAB51CB8A3177B0AF2F386B685306A21591F3E2C532FC9066857A72 19277BBD9C76CB315B78F76511325731
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C

10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	F88FD78260592477776B6820A2B8CFC77C73BF4D0D01727EECE8A1D3E68A70AB459E0A6C768F219E874C18D773646B5BB
12	V	03FDABE45570FCF90E50C569300C5B82EAC086B9FCF32304D7ECDABB94131AB04AEF96B0F3F21FE13BD41DB9A61BC590
13	reseed_counter	1
14	output1	CFE2F4752F2AB45473D1784B9498496047C3590522F64CECF83B3FD588C3B3D8E79D6E6B8142BEB3B4D5AB1B8904DC04CE9D485723B9A71985D2C359713C32E29AE7A404512DAD22F8F26FF4C5AB476BDA775434F5D864E9031DF899935B3675
15	Key	CEEAAF95BBCC5208691CEEB542820F4995A232E764C636379BEB6DCB9EDCFA0102818280E6971A4EEF64FFAF951E87CD
16	V	3F9B63B7761D89382A6674A1C34FBB4305C738C9809F839EF49C398CAAD152BD212AAFCDB479BCEF21CEA8CFFE9FCEC2
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	0A62BE887D7CD740CACB47FA91A27B98926519F6E3D4A1D334F63DEFCC3E2F9E742B5262A66F32FB5A7BABB177EDF4CA
21	V	06C653312B28DFEF12558162840B39A2078BB38E2D733ED80756500217100C5842BAD3089886575456ECFA1FF54EDC5A
22	reseed_counter	1
23	output2	3E76FD980A31AC67F7C5988E5E884379D4AA916B99AE2C637FAE523B7F23B05F1688B84021C538874A910413B2273323CC7A6424D19545A0D6358017BA11C0DD2624A225C3BDDD0C86B8D305267A09E2D1B23D75A48DA979CB92FE3E8EB4F44D
24	Key	6F6A216F53FB946330EAB14EC5A271730545DC370617FDD638B386675FA3D7F6B24AC33A841E282C7AE22CC18D8597CA
25	V	B717350504B6BAACC0A5D3D843A9D3C2FC84D3C1F28784B2EE4BD646B4E07238A34F044568F7379610A30B55477D62FD
26	reseed_counter	2

7.2.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405

4	Key	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101 0101010101010101010101010101010101010101010101010101010101010101
6	Key	03CEEDF46432B9FAB1D8400BE97AFB38A8118B793EB9ECC00F3BE53163741EE5 B0EE7B5327697E26E0EE8D426AA1A8DB373F4A1D1B8402A141AF5C18685431EB
7	V	6BEF9B37F8265CCEF1B84CFB21284B8ECD9F4166B2FCB3E93B3A262BD9D0788D 5A4B236E808E125C5880591D545A73CBFCD9050C7E080789BEA38AD5F4C11432
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	6898F13B8816409AEBE311370E38E07FF12086879A6148438F4ED3EC89937E37 6EE0399BB29E0322F26EA284BDE3EEC82B4BF3576492168FF6F98B08A3A3D136
12	V	C865D2DA248113E4FC46FD8001A86746F555B4759FF6ADCDC77E6C1B5626B198 E77933D4065414A0AFA0D6CD0C3EB8BF02F48DA911C16BBF39F1D21C9ADF5B6D
13	reseed_counter	1
14	output1	2BD06EA61F06D0665A38B19162CB2FDB71AAE80CFFC978AFDA6932A1E66C5AC9 CEBD48F3A4BEDAAB8EAFD1B026F1C64836A2649C60928F967717DD3120C46F46 780CADF30EDAB14C3296AAA01482FE58A10713B755E25A995AB260985595D178 9D2D5E5691DD5CA952C432E1639932E027FCFCB52A34ECDB7B899FDA22E02577
15	Key	87A7337F5AC0013CD31FDB1E8739BC850229DAA8F8AC974C76A476C22FFE2906 EEDE6C9EBEA12B3CF38B92067750220024690BFCAA23AE612D6587ED4131AD10
16	V	6159C595D433FEB59CE999B799AC3FEEA7F204CFFD6EDC8D384E8BA932937F2F 8021B5D1A5C7B7EFFEF0FEA5C8A9B3904539EEB1027345F793A3C8292C7978F3
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	49D892059BC2ED983A15B89BF5C86BF256FC2D39E60E5FF0A3748175DA76B40F EF4DFEACD31A6A0300A8BCDA34FC1B0EC67478F99E3196D464B526869CA5B9B6
21	V	0DF60D47063C905FC4C3D638E6F883B0383892B1E9C9EBA579BB3CBECB9C0334 A4DB2DA90AD7DC80AD3D32455255693D93CE05055954D3A293F8F27CE8329F2C
22	reseed_counter	1
23	output2	6D46E3037FD3697C95D19819CF6A0EAB8252121CF308542DB40BA21DA65CD293 F40018DAF6150B07652C688F29CDEB743D7CD7D7295C4B74E15C3514FF729634 3276F274E8393D94FA608A5A2361743B7C1EEF25F32EC58CD84DC2AC0294CDD0

		A2DF3150CCCF1EA1DF5DFED3ECF1EBD3843CD171B0021CCC493B012EBEF17E37
24	Key	B1140671069A07E2FFE1E822726641357C76EC60B6DFDEE9AB01AEF67129ED42 E76E449DC541A81475FD6A96989DC91AD64C72BA7EDE0C314AD8476F67E2E487
25	V	A86857F6F391AD9D2A9992A3CCC509242ABE23D8E6C02523DF979C398E050A17 3BFF5FD3F818BA10370CF477791814FD4F3E88BD3194FD7596364C70CAC4FDC8
26	reseed_counter	2

7.2.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	E142209AFD9E77D264030161D7EF1C423DF7DD444B9A770F5B9629AD
7	V	EBAFC5112C43CCA72D92C8060AC5745524EE2846A1E759D2A98E3EBF
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	0484C8653084EB5641EF6A433397C321CC6C8FCCCCA3B4A30BF13052
12	V	4DBA51F1F5FA56E874B6191552189D27B47A108906BEAEACED9AE0C0
13	reseed_counter	1
14	output1	628A3BACD0A290921D42FA3D1DBAC1031F1FE21CB864544FBB5119844D67A11E 0A1C45D61A423D909AF1C1B420370E015E296F44BF83B26A
15	Key	4FFC9291F6A601EB5DD67040A5776573A9D3CCD97415E513DBC28739
16	V	0469B8FF5F27E785B2F9CDAF9CA96BCA2825CE87739851 3D3537CB4A
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	D67CE547053FDD9D8D615CB0EA188D7CB64B11E05F551C5B0EFB09CE
21	V	A2558FF643D3A9410FE28A2282539F96AFF566B3C11E22D99DDC1765
22	reseed_counter	1
23	output2	8000FE254D953A00EA6BBB497B05335576BA5B36B78D2F392FC7EAD517F167F8

		2245446458O3CFF9A1AE8BD3738679539BDED3B4EF8AE75E
24	Key	5E36F9A89E62EB300934DA525A01B6996EEF47DAB84D91B4582D47E6
25	V	ED0C9A1E0C04D1E50336EFAAC70B8CBCD3985C01A2167C22233B31AD
26	reseed_counter	2

7.2.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	D8EF3FFDAF4157DBBCD84380AA38A9D30F7C4818F0E9D6100E2107F5D870FDB5
7	V	B4F20FD25FE1966D249472E51927624EDFC76548A61A75E77A1741EC65E040A5
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	98F61CC6CA2D34C842C6DE63F9374C9C325DFA0F04B3FE99ABF8A0B30690A704
12	V	55AFD23BD06030BF29731686B0CB9625AB1773A26772D85AB188B84355C99AE6
13	reseed_counter	1
14	output1	D77801E5A5E46A419D62E56F0F7C95CCAD3E4F9010E624DC2D5BC32256E5231E CB5FDF3D652C969EEDE74AC5F21859C265715F7CF975FE5AAD0B5FD42A166822
15	Key	C82E18BA9BBFCDABC028D42CEF7343713CFFDB67B86B6002A388578547BA6AF3
16	V	A6A8BB5A0D83C9D720E73F50F08D69F73E59BC183B174410205839F7B110B170
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	F99D7D60B7B437F2C675B10E9092D1B5CA541A97CD8C1B34395E8A04C9EE4872
21	V	140F015309D4F83A862DC1E2B149D9029000A00942C1044C6A661CEBC577A614
22	reseed_counter	1
23	output2	2296D7CAACDE834674EEF90E3E7DDACB34D3CEAABA457F6C58CCFCAFD86550B2 BB508967D1A247ED969C55C01AC8D9012758F70787A480F0038F6514F15B3219

24	Key	A24BBED856C001C5CE03A82D6BC60BA7659927D0CADBEA8F22197F404D127DE8
25	V	8EB782E1F10824669E5A19C1F7592BD961DA17D86A1423501D1AA3838FA8FE5B
26	reseed_counter	2

7.3 시나리오 3-2 (개별화 문자열 미사용, 추가 입력 사용)

아래에서는 시나리오 3에서 개별화 문자열은 사용하지 않고 추가 입력은 사용하는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

7.3.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	E747263F6ED232DA1B788D1DD8A0F881DAF9A8D8B125B19E6077943108063 7DBF555CC1760C9578E1555454D55F1A60FAB898A1DC493B7C0
	output2	CFD68ECA772D8E75CBB1A49A1A7322A440B7642B68630D7347C352970E2CF3F2DC551C6FF1C1EC1B1ED5B706525F4D59FB224A639E99E176

7.3.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	69821F6AA64080773455631 38FFD475B6C43F24F101FA3888DFAA264C4121F83A8CF8F6B86FF45A5870194BB872762E57992F408FBFE890BB0FF3E65A4AF48AC
	output2	07D5337D708679E2F306DA49EE61175002552D24359DCCAD59D5B497FB53ADE68142BEB886755CD6D9817F4DA3525AA2D056C3399573C201F6851110C8ACB15E

7.3.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	A7B479513AA9BC8DC35A3574D4847717B73508D8075CE3414815596F80573C359D23F56784501ADAF44F50C68C8AF2E581124016EAA933F61C8730709BA8582F7E2F96CE4807301391327716 6AD97C2ABC205E9243A2872432C3C4463D2AA960
	output2	96901D3FE0093361652E8DFFDA6073165771275 26E5B0380B48A259D372B8C6B05A71EE0BA57AD4D5C4540E49252AA28584FC25E39BAFF80936E2A703FFB15EAD5E2F6A5EC7E9410 12D1C30FC07875491C5D9E7A8A5344E1AA608B4748EE7B5A

7.3.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	E505297C89C1A007E14C01A0C861318D3857605588D73DA041F223758CAA4DC6C5322AB924F8F35B21D1051649DF849CE93743D72F759BBF59F014C40F90EF81DD95B45F1EDC50A61CF5DBA24B5A703AD3E9412FC7426DE10F7514674577AA09A5478B7D7D82FC5CDB2B0A4F0345ACADFE1B9F171A5AE3CB0832E6CB788AC24E
	output2	80DF3B344FEC48D656E1E357336822E71A349C6DAC4CBA97301E8D25511E88FB48EF836AA5A09A5B0E2E9D0B7631C5572E4E0392C2D6B5A5ECF4663101F9DB2903B7DD1678B6BAA4160098D57A2631C0E4D64DC5410FAF05766890DBF57F30CD9E0CF136D77246622A58CC3238011CFF52A21CC7BCE5FB1F0598860D26018B48

7.3.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	B7F64771E0EEA547B071E59FEE30E7A587F80A2884862FEDA2641CA82472A774 6C10EBC40558841DC158DD686C41696FA7862A5B963DC78F
	output2	A32BF42A91FC66E3213695382O4C4CBAED6386B354421DDB0BA3E35153022545 C19652F35790C12F0AC853B997ECBA1C39C6B073F1345889

7.3.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	679431096E0CFC5403872509D3E19AE032EB472EE9B7168BD4375B0537DC1BA7 5BD77354CB194FB68A6C09EB93AB11D61278E8331FEF340807D5D1718A39227D
	output2	A7CCEF87E52090B4C24C6580D20D51D46C19C89FFAF719AFB6D52FE81B5285BF 2A17B944FC18E909D91C10B997F86ABE6D4874121134FD0FE78653C8775202E4

7.4 시나리오 3-3 (개별화 문자열 사용, 추가 입력 미사용)

아래에서는 시나리오 3에서 개별화 문자열은 사용하고 추가 입력은 사용하지 않는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

7.4.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	C7CD281CC07E766D5487630BF4CFC51F58D9167D93B538D205FF3E31E411846609517DC4DA64C7C4F7ECFE36380D59E7E6DC533BCA0492E6
	output2	7D20BA7ABF4C7C5D948F50CCD571D444236D9656D8ED9808E7E0F69BE319B2FC29991C8D31E59609FCBDFAE3CB9BC34700BC924D3444CA5F

7.4.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	C4215097A7AF6588DC4F7F993C92A8DC23868097FD12584576BFABAB7B23D2A6AAFCAC1B69CF9043F0A4038B003A466D48BC837A077D9F38D474A677055D8AC4
	output2	C092A1060DB2467AFBBBDCFC530CE1E23C47D02FDC5F11ADE78FCBC9E9C9E98CFF971F504115688FCCF0D8EB882B54ABBB6E1E1A6C2E27776795589137400 3BA

7.4.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	DCE12C0128E6D7E0A1AD608AD4B19E4512AD85176C8433A86ED4B7B6CD61F3A54EC6A3E39FB4C2CFB852980C6DDA9F5C62E731626D92873479E1220800B38C5FD31768758108328 8B9F770195CC190692A72678F6EBDF850E1A3F3755C85A5C3
	output2	5339E4345C0F1B3D4BEBBA824CE5DC3277982EDD3785E276B202218BA24AFD49750694DDE06E60421707459526A2FCAFA71E5C2B299058405BDCE16900A5DDD3D7774159026390E87053D4779DA5702C3BDD67B123C73A9B23CC331B776F9777

7.4.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	DBE89892F7125A3F572FAB549067E2C50558DD2C848EDD487D090C31E582A9086E1CCB9853C0BFA4F518981782FDE7046D28C9553B145D5DF15DB95A719FF2C5B75591FB2957E5BC6629AA3C316738FB9A1003D5BB3CAC311290E607F165FF4823E84AB65F14E4DFF0305B6FC71B99A47EFFC9F30F67539873A5889B3086FC73
	output2	0F3F5875D16D094EA8D46A84F72F9463F92E06CDEB20C1198582C5348CC3796A6DB7658A940FCBE908E09471CC92FAFA4334F342F570215DF29CB5F66F66AC5F45C4EDDDCAD37FB32DEED447A7AB3A9A47271EF2F3D9F2A9AA6B14345FE170D9A23779EA32986A29C6AE39B52F44D2371E550B6DC270143757A36A5D0C944968

7.4.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	C22A37156BB973E6C1B51318E45D446BDDF159BFF96F82BF4EAD3D527ABD226118F88D491B8AFE3B3934F31894A88A1808BF85ABDD80BA90
	output2	6DBB1ED87277B606A50ABDFEB7B291766A7E6918A4C0CDFB75C68710BD69AAC34516815C606D6FA3753D35A0065938AAADA993B7F1DDE2CF

7.4.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	12E752DF1C7EC5044B3C47C5F98ED9ABBC517C41E3B08DFE5EE9040150376CB1EDD9C28B5ED2DC661BD93356BFCED0248CDA78C7F1EE6DFD0676514EFDA19F9C
	output2	4456FDE924468C01B27718C67E632BDA3B09D33E65F24D961AE1C5A9F60115E5CD2AD86C70F38ADADAE6C540874004A0D30A7AF8B1A7FED144AFCA9D50D891A5

7.5 시나리오 3-4 (개별화 문자열 미사용, 추가 입력 미사용)

아래에서는 시나리오 3에서 개별화 문자열과 추가 입력을 모두 사용하지 않는 경우에 대한 HMAC_DRBG 참조 구현값을 제시한다.

7.5.1 LSH-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	6C26E31EF29236508D687AA99FDF83F1270731248A598944951439EBDB603A4D0EFDCAF30B6524B71473A40A102D1B557E469A59654490CC
	output2	6335A1382EED59BA68EE7B5D99AD620BE303FF3B0C2C7BCF105158013B964804F2824E5467E6CAD3F401C952B44A90F0750B4F2B4E98EBFE

7.5.2 LSH-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	09B400A2445DF265EFCA578BDF6C96B934643222C903EAD25802837348F992DFDC18F4470B1C25A74DA60EF6BC9C525D0DB1C3E0E04912EED1324267686DC484
	output2	803F35331ACB64D11689380E24C9587B5BEA27D8F0B55973A7FE176B4922571E00CAE9B4FA19C7E8ABF0143C55B46400128D31E589897CE9DDC1052DBCA4A088

7.5.3 LSH-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	3CFC83412A9BD5437CD5D0B827CA82BF813B1A655E528D001D6328B67C0617FF640DEF9A863E459FDCF6A19196D798FC39C98C19B5BAB7CB33D979D024B3A0637C065457812786919A3836C79EFA36431A7B442E6124E8F10DA76778F7FFE3FD
	output2	2B735E3160C5F567370E4C2D2B0AFC5AAFD972B5F69758C4577DA1AF0B2CBE4A34708E422967E14EEA95B1AE452E7AE43DC96DEFB2CE73F7B60D968596D47F6DA055BF3ADA9AB3C5DD069E1E16B633A60F2097F88BC072D02DAB7D9FB35146B8

7.5.4 LSH-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	AD6D3190D72C66D97B330A2AD3E79E6402F5C02B76FFECE49608841F4B8B252F3031C008ECBCAFEFC7C15E79BA67C9CD38F4555CFD2CF30FA7783FCDAEA3CF950AA1A192720E43C1D98BA69033D7CF6B1311A75FBC44749A6577CD1C74E15019CD0BE9471C6B8E02019657B8071192C35551082B5F8D4376BD98F312F889FB47
	output2	D29D72E401C019FC6E50FFBD7C821EFE257603BB4007F30063B143A992591F1C8F270B4272C5EA831CD3161A7461083D56D06E76F8A267B43BB94546F6C016D2F4A039835ED8D3860BE39BE41A4A34ED357DDCF0F0150239250982FEF142B885146278CA2EAB773CCCF8517AA9916344AB8AE6786D96D2FE7C83FC695A7D0399

7.5.5 LSH-512/224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	EE2ACB46558DCFDF0FD39355DE8BC5B9C64B8BEA7A16A9F1362B88F2465E970B 8A45868559DDCE97DAD19E74ECEFE58BED069AE19AAAD54C
	output2	06D2BE40D881B97105C327D163CD1374AFFAC6EFC8588FE7A4014D50DFAEFE1D 8E01B7A24F762F4D011D08D4B49BEB24D9DF9A9B568298D2

7.5.6 LSH-512/256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	0C6155D76CCF81DD464F3DFDB7F1009E64D606F5BEFAEEF0D61F831E1E269C45 4896768D52F5BC1951C8DC9E4F83CB722C17C93150E2B06E1732BA57C1CE1BB8
	output2	1771A49243EF37AD33CE3FD5FE5034C47A11E7F55B713F902F7F54C429DC3829 C046F1A809B2A63306A32856A8AC906686DC83F7F9C4A4BA30D4BB592072DFA7

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] ISO/IEC 18031, “Information technology - Security techniques - Random bit generation”, 2011.

[2] ISO/IEC 9797-2, “Information technology - Security techniques - Message Authentication Codes(MACs) - Part 2: Mechanisms using a dedicated hash- functions”, 2011.

※ 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-Part1	-	정보보호기반 (PG501)