TTA Standard

정보통신단체표준(국문표준)

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

해시 함수 기반 결정론적 난수발생기 - 제3부: 해시 함수 LSH

Deterministic Random Bit Generator based on Hash Function - 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 기반 해시 함수로 사용하는 DRBG 메커니즘 Hash_DRBG의 참조 구현 값을 제시하여, Hash_DRBG의 구현 정확성을 확인할 수 있도록 한다.

2 주요 내용 요약

이 표준은 Hash_DRBG 운용을 위해 고려할 수 있는 다양한 선택 요소(예측내성 지원, 상태갱신 주기, 개별화 문자열 입력, 추가 입력)의 설정이나 사용 여부에 따른 내부 동작 방식의 변화를 반영하여, LSH를 기반 해시 함수로 사용하는 Hash_DRBG의 참조 구현 값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 TTAK.KO-12.0xxx-Part1에 규정된 DRBG 메커니즘인 Hash_DRBG의 기반 해시 함수로 TTAK.KO-12.0276에 규정된 해시 함수 LSH를 적용한 결과로, Hash_DRBG와 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, Hash_DRBG, used as a hash function based on LSH about implementation conformance.

2 Summary

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

3 Comparison to Reference Standards

3.1 Relationship to Reference Standards

The test vectors in this standard are result of applying the hash function LSH specified in ISO/IEC 10118-3 as the hash function based on Hash_DRBG, the DRBG mechanism specified in Part 1: General.
And, Hash_DRBG and LSH conform to the specifications of each standard.

목 차

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

1 적용 범위

이 표준은 해시 함수 LSH를 기반으로 동작하는 DRBG 메커니즘 Hash_DRBG의 참조 구현값을 제시한다. 참조 구현값 생성에 사용된 해시 함수 알고리즘과 주요 Hash_DRBG 파라미터는 <표 1-3>과 같다.

<표 1-1> 사용되는 해시 함수 및 Hash_DRBG 파라미터(길이 단위: 비트)

해시 함수	LSH-224 LSH-512/224	LSH-256 LSH-512/256	LSH-384	LSH-512
블록 길이(outlen)	224	256	384	512
시드 길이(seedlen)	440	440	888	888
N	0x000001B8	0x000001B8	0x00000378	0x00000378
len_seed	2	2	3	2

<표 1-3>에서 N은 시드 길이(seedlen)를 16진수로 표현한 값이며, len_seed는 Hash_DRBG의 유도 함수 Hash_df의 고정 길이(seedlen) 출력값을 생성하기 위해 필요한 해시 함수의 반복 횟수를 나타낸다.

Hash_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 1-2> Hash_DRBG 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 1-2>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.

<표 1-3> 부가 입력 정보 설정에 따른 시나리오 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, “해시 함수 기반 난수발생기 - 제1부 일반”, 2018. 12.
  (※ 이 표준의 용어 정의, 약어 및 기회는 해당 표준을 따름)

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

3 용어 정의

- 해당없음

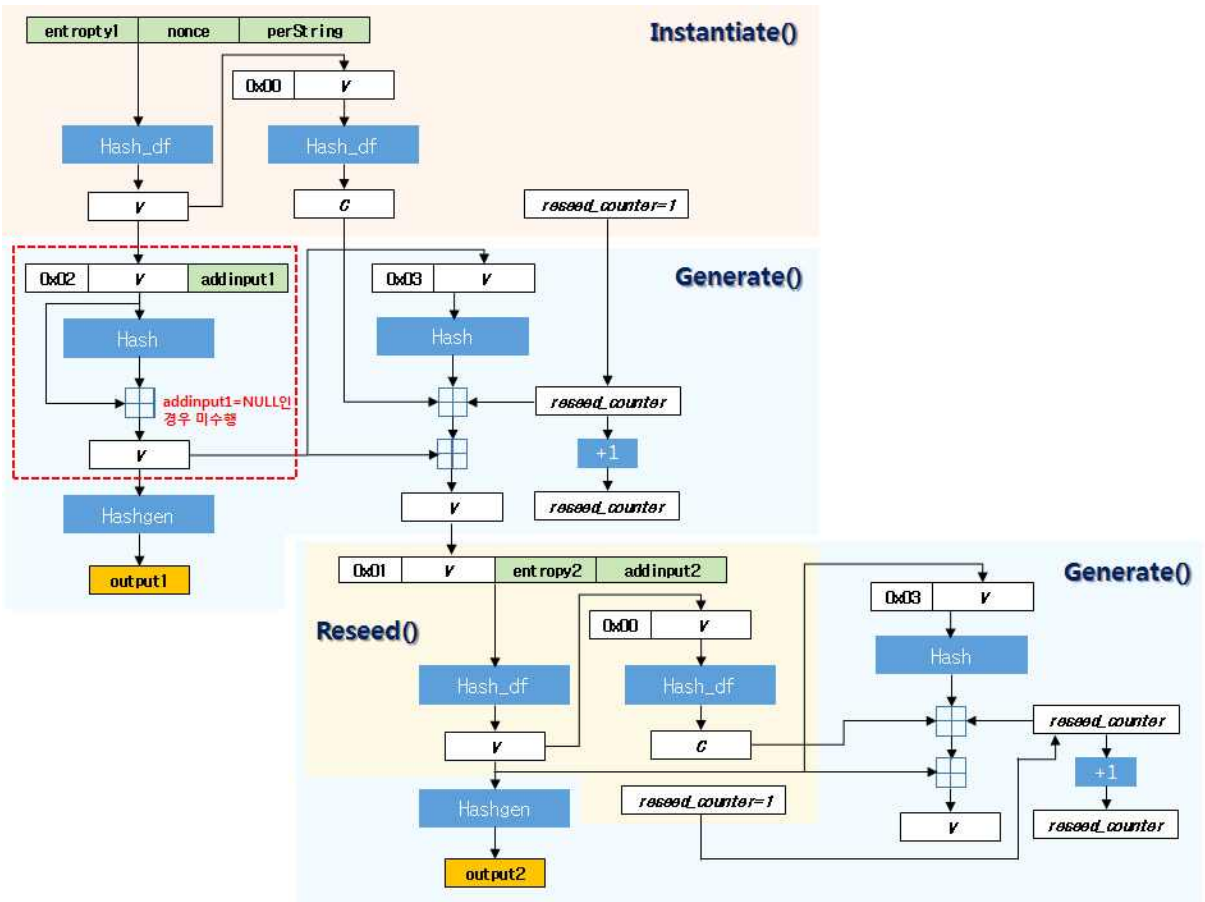
4 약어

- 해당없음

5 시나리오 1 (예측내성을 지원하지 않고 갱신주기를 1로 설정)

5.1 개요

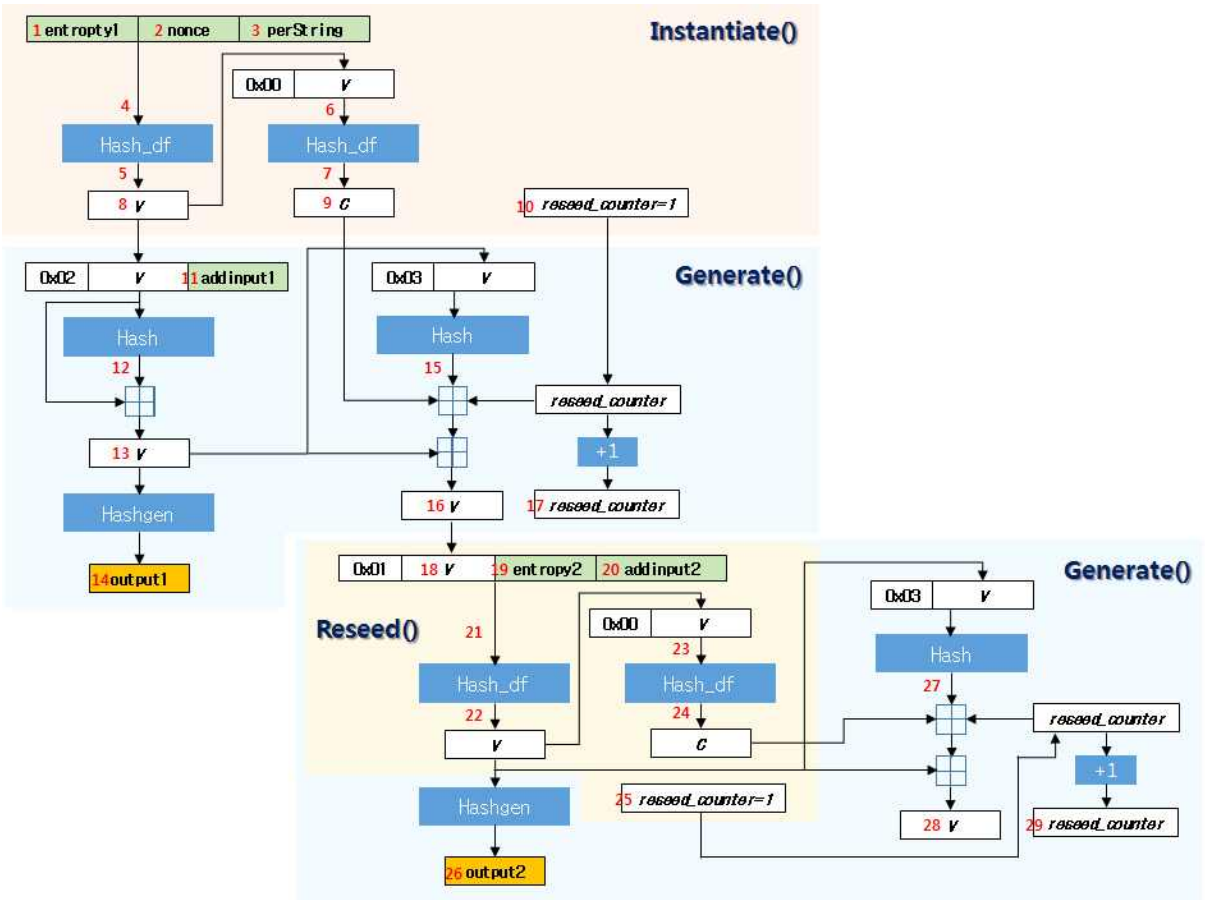
시나리오 1은 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 1로 설정할 경우의 LSH 기반 Hash_DRBG 참조 구현값을 제시한다. (그림 5-1)은 시나리오 1에 따른 Hash_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 5-1) 예측내성을 지원하지 않고 상태갱신 주기가 1인 Hash_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 LSH 기반 Hash_DRBG 참조 구현값을 제시한다.



(그림 5-2) 단계별 참조 구현값 위치

5.2.1 LSH-224 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD155198417 53BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD155198417 53BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E663 05DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D

6	dfInput	00023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E66305DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
7	dfOutput	4126A8395AD8D221D183027BC02A1A773B8AF98F0AD66D946F799391F0134944A603AA7D8DCFF7726EA2A91E157E02A6F92B10031F9486
8	V	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E66305DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
9	C	4126A8395AD8D221D183027BC02A1A773B8AF98F0AD66D946F799391F0134944A603AA7D8DCFF7726EA2A91E157E02A6F92B10031F9486
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	FA920888ED46415195311AD5C1417455285E63B60187F10ECC87ED30
13	V	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7E1B1EBD6F504C1DF73F869EFDEBA0BA52301DF7E61784B8BCB86C1ACD
14	output1	3C8436BBDA0084585D66B05F5599316A05FF0C273F230C8EDA258C981A42744DDA45FDC8067AD4B514712C6187FE6B4FE783B192B3A99A07
15	H	8FE291EF003FD9043747D16D4879778F55C0D183651B6BB48CE036D0
16	V	43626552076E1AEFC25603CC6E016BFA69FBE5159CDDD23C7047123CF162A79531FAA5F45C4062A688D48AA3F4476C23994F81486BE624
17	reseed_counter	2
18	V	43626552076E1AEFC25603CC6E016BFA69FBE5159CDDD23C7047123CF162A79531FAA5F45C4062A688D48AA3F4476C23994F81486BE624
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	0143626552076E1AEFC25603CC6E016BFA69FBE5159CDDD23C7047123CF162A79531FAA5F45C4062A688D48AA3F4476C23994F81486BE62492BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	1890A0C6E36EB628EAD2FE353420A092C00BA493DCF18F0B03954E9571555BD072A79CA8644AA7EC32A336AF729662A4ACF3FAF13C351F
23	dfInput	001890A0C6E36EB628EAD2FE353420A092C00BA493DCF18F0B03954E9571555BD072A79CA8644AA7EC32A336AF729662A4ACF3FAF13C351F
24	dfOutput	1D48C1A2308F3BECD582188CA47F728493ECFD5CB0AE7899914A22613A6D55CF5F3B8A4D0B6F600DD74EAB2ACBA61D0DBE90030CC04B43
25	reseed_counter	1
26	output2	C774B570FC99A8914703B314FF90EB9457F7D92CB48FADDD741082C0BA863ACE

		E28CF3ED1DC2F72E8FCC84968F69F0AC8276A7C0B9F5B085
27	H	B2D2C601186CBEF1A83D8A9F2C3F5750E6CFB7D4E050FBE07E6A18E7
28	V	35D9626913FDF215C05516C1D8A0131753F8A1F08DA007A494DF71A97E88B2B8 3EA2189DAD44A726494932C10DF45492BC7FDE7C66994A
29	reseed_counter	2

5.2.2 LSH-256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AE EAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
6	dfInput	006B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39 AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
7	dfOutput	9D6B66A8636E1B65248705B2DD0CFDA1A0BB594275022EB49A8B35B57919FCA9 CCD43D316D95B300340815C46DD47E9DFF600C75631A61
8	V	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AE EAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
9	C	9D6B66A8636E1B65248705B2DD0CFDA1A0BB594275022EB49A8B35B57919FCA9 CCD43D316D95B300340815C46DD47E9DFF600C75631A61
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	0011F71DA9E5159A7378EBC73F9475CDE53EE9F013255385CC000D80D571D5FF
13	V	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CE1A0BA970CC4D422 63E1E3E0F28EEE19164744AF3DD9A3CFD8A238D102CDCA
14	output1	3BE9C1A3C3DC9F57C57ACAF36A54F6F9C3A28CF6D7848540D88A9DC31461A927 9F6B45AEAECF9AD81E43B1EC674ABC0EE57347E4392D270E3E0578A99252F41E
15	H	0365C0CCFD5E91CFAD573FD606E7BA621C8BBA4016B3AECED4CD4CD455E8B07A
16	V	0885ADC3CD32E49010622736EEF25199097E6C3AAE6775D4E1ECBD49E470A079 87F5F71947DF0335D6099A8A5F5CF142A54F199C4E98A6

17	reseed_counter	2
18	V	0885ADC3CD32E49010622736EEF25199097E6C3AAE6775D4E1ECBD49E470A079 87F5F71947DF0335D6099A8A5F5CF142A54F199C4E98A6
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	010885ADC3CD32E49010622736EEF25199097E6C3AAE6775D4E1ECBD49E470A0 7987F5F71947DF0335D6099A8A5F5CF142A54F199C4E98A692BAA7658C23A7EE 8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F 27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	8750B58073156F776F66A9DCA68EBDCB2CC9BD7FD7F4A17C846FBB10A01655A0 FFB2155120197 56FCEAACFB19B8251E2CEE75B6DF54FE4
23	dfInput	008750B58073156F776F66A9DCA68EBDCB2CC9BD7FD7F4A17C846FBB10A01655 A0FFB2155120197 56FCEAACFB19B8251E2CEE75B6DF54FE4
24	dfOutput	717BBA297EC9AFF30725D125E3076DC930B405BB92A9E92F02BA27C25D31B824 29F7149533CD5540F2D1A384FE49B08B2F75C0721E78F1
25	reseed_counter	1
26	output2	73EA82F590C4E11E3EFCE8C2E91078647E1D52BD54F082568FE042B40CF72006 9118BB436488032C9DE4230B80F1FA2669970C7F17B807D7FC46BD22535E1586
27	H	D14AD9C164172AA34099B40E2A9EC3A42974CD2B9C619D3289E1D5905FEFB32E
28	V	F8CC6FA9F1DF1F6A768C7B0289962B945D7DC33B6A9E8B7CD203A4371472B105 C35D3810F2AA6EDA36499ED2FB6934F7E032AC40037C04
29	reseed_counter	2

5.2.3 LSH-384 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C2 9264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0A EC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8AC

		BA62997B7BEA6A975D6D256DDCCFF1
6	dfInput	00E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF1
7	dfOutput	B5E5365A977CA11A5AE9D0EE37A325A920316E2C37726E6EE98A4ACA53ED64B919A69356D639A679D0877E2467939B429676EC676A303F1018A965B21C38672AE85099122EE5826454764D629E1318948BA67ADE9DB7E85D36D4331CDAF990A7E3FADA75E59F144F9D643265ADF07D
8	V	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF1
9	C	B5E5365A977CA11A5AE9D0EE37A325A920316E2C37726E6EE98A4ACA53ED64B919A69356D639A679D0877E2467939B429676EC676A303F1018A965B21C38672AE85099122EE5826454764D629E1318948BA67ADE9DB7E85D36D4331CDAF990A7E3FADA75E59F144F9D643265ADF07D
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	E8D69C9136CE8A49675FD83A229217152948B077AE40C6251A878F2C61EC3089ABDE71FCDF0C01C6061F8133D7A42D1D
13	V	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575FF3C2B70C20174137667DC17B865FA557C0E3B64372CD2C67706AB7C73EF287525898D4965A87EC309D7CEE594580FD0E
14	output1	1D8B23825439377ACB4E7B6C5EC4F573C039BCC07522916DB7C295AF6B9A136D800F23969C3CB2D01D0D780A7A1043659A843067DCD8D93334222E5CEBD1B794336C8D3AA99B3572002E7F7F17AA87B9D9EF8D64B693EF0E2F8B21582070388E
15	H	6B50360DD2EF6C409000299F771C68B462B8BE9ACC4849DEF46612D47674CEAA4B7787A90D332CD5070CD8084C5366FB
16	V	9A6348064E378B88CB8F56DB4AAC16B8C00791317B6A35EEA8C4BF325AC98E7BAC0B5D17D3C95863B3B3012BFA8E6CF594FF4A6BD334068654E451D0FB8FC789FB3DB3053592FA5AD26168601A2124B8281B591DB32E2EC2079ECED2424F8D4BF45719DDA0B819F4272A93F7825487
17	reseed_counter	2
18	V	9A6348064E378B88CB8F56DB4AAC16B8C00791317B6A35EEA8C4BF325AC98E7BAC0B5D17D3C95863B3B3012BFA8E6CF594FF4A6BD334068654E451D0FB8FC789FB3DB3053592FA5AD26168601A2124B8281B591DB32E2EC2079ECED2424F8D4B

		F45719DDA0B819F4272A93F7825487
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	019A6348064E378B88CB8F56DB4AAC16B8C00791317B6A35EEA8C4BF325AC98E7BAC0B5D17D3C95863B3B3012BFA8E6CF594FF4A6BD334068654E451D0FB8FC789FB3DB3053592FA5AD26168601A2124B8281B591DB32E2EC2079ECED2424F8D4BF45719DDA0B819F4272A93F782548792BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	df0utput	BFA6465403 18EB3EB00E73E3C7E07467448BC00C97EA936D7DE444D772440 23D6645E9122D087F374EE0EF35D1EAFFFB8CBB9F670E87918A0505A74DD076AC32D5648D74B4E0E9DBB3588B8E71A988DD25B0F0C70E25851A9778E19E63E17B6807D053D3608F835908CA3E9EDA8CB5
23	dfInput	00BFA6465403 18EB3EB00E73E3C7E07467448BC00C97EA936D7DE444D772440 23D6645E9122D087F374EE0EF35D1EAFFFB8CBB9F670E87918A0505A74DD076AC32D5648D74B4E0E9DBB3588B8E71A988DD25B0F0C70E25851A9778E19E63E17B6807D053D3608F835908CA3E9EDA8CB5
24	df0utput	E4BBE66F52592CD4A7D1B6F576FB4C42944D9AD9124CF306223C4500B29579A723099C470397FB88220DEBAABDAF56811A830892C431049A1836AE5D28C1E42A2CD413278D99EAB6858A1E0D189887421165089A2747FB2335032AF33859FE4DF0A9AB86901A77FD981A4FEF2DF3D3
25	reseed_counter	1
26	output2	61838772FA38232D3232457484 44DC273FB8CBD2DBC910B742E9978C98A6437C50F1611BBC0999ED99737759411C593C3F01054EDFE352FEDF38D4B35D72A912BAF3BDA193DEE4F9F82B2F55A9F90E6CA03A18BAA500C88D6EDE065D7C697EC7
27	H	9EAF0FE3D1D5D25C57C3F46714CC77895BD276E2AE7FF18DA15FDD95970B28644794CF5D86F39C02D7DAA4C731615A83
28	V	A4622CC35572181357E02AD93EDBC0A9D8D95AE5AA378673A02089D824D97BE4894F855930A07ABF70EEDAE08F9A567CA73EA7F9D2B896241D3C55AAF93890FBB148846E184D30E9FCD710B056B9997B098CDC0FB55F0DDF2C59A228A763DDFD8D495CE0E445FE2E7B8955BF69DB0C
29	reseed_counter	2

5.2.4 LSH-512 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21

2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD 72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C 92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF61 9DCE974E8B63E92DCAF22631399B5B
6	dfInput	00ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916E AD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A 5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF 619DCE974E8B63E92DCAF22631399B5B
7	dfOutput	BC1648BB27119BABE1D09A426BBC66DA6FA54C1C432AAB80F46C0645492777 13 85705036AD4986F0FB0FC73FB1C2F7696256EE93B213D25DDD556D0DEE90E0C5 EB74B3DFA65C99FDB60A367577CC06FFA7AAFB496818FF2462F12028B691AEFE 8DAB3BA702FA2ABE9C7D5FDE6A1F2E
8	V	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD 72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C 92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF61 9DCE974E8B63E92DCAF22631399B5B
9	C	BC1648BB27119BABE1D09A426BBC66DA6FA54C1C432AAB80F46C0645492777 13 85705036AD4986F0FB0FC73FB1C2F7696256EE93B213D25DDD556D0DEE90E0C5 EB74B3DFA65C99FDB60A367577CC06FFA7AAFB496818FF2462F12028B691AEFE 8DAB3BA702FA2ABE9C7D5FDE6A1F2E
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	4E8B7E1E3B2C9948770C7B4C3D980F2F7958F585DDC940CAB3A6C9763308B4C4 74A6D94B1A7B6A68789455BC47B845479DA7A5B30C4B6C29264F2ECEB58505AD
13	V	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD 72D32ACDDF2F26F3A454F0006389305D0736235A6E579F9194228C294C78B9D5 EBEA8230EB6376D2EF537642D7C612F2D5E1A37751F2213C8A6ACC98E29DF6FF 45744A5AD6D012541A20F4E6BEA108
14	output1	6B51E02F8C250DE36439915EC8A8A80996A8B21ADF45DB32F7BBF86942D16F82 4F2E8C0F6F1B5D9C3511F3262D69547585D5240036E4EEC041986B41879A837F D5717E9CCEDE03DFD2F6092165DBF3E550250C3918E0B7B4DF8258E963DF28AD 2882825564901 9DBBE52F1FC82862D33FE431A51951CFD618B730EFC88C39CE2

15	H	90F0F08FDC65536E4E17C38D1B9FEAE4DAF115155153348F51716B7353E764B7389B41FCC9C142D7D74B222BB4FF955ED1E72D73FE311CFC50A0CC4F4C74D63C
16	V	A97B48A3E7FCB4DAF808659C3E69AB4BF83A7B3B01851AB9E8E1BF9F64B8E5C0F8437B048C78ADE49F64B740154C28575A7DA1CA85BEE03D893B8652DAF47F76C8744B61E4F4A02216C9200C36F6D12B18CE9B8A7B4DF838387E187698C504CFBA4CFA000AE73963576AA4119D9673
17	reseed_counter	2
18	V	A97B48A3E7FCB4DAF808659C3E69AB4BF83A7B3B01851AB9E8E1BF9F64B8E5C0F8437B048C78ADE49F64B740154C28575A7DA1CA85BEE03D893B8652DAF47F76C8744B61E4F4A02216C9200C36F6D12B18CE9B8A7B4DF838387E187698C504CFBA4CFA000AE73963576AA4119D9673
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	01A97B48A3E7FCB4DAF808659C3E69AB4BF83A7B3B01851AB9E8E1BF9F64B8E5C0F8437B048C78ADE49F64B740154C28575A7DA1CA85BEE03D893B8652DAF47F76C8744B61E4F4A02216C9200C36F6D12B18CE9B8A7B4DF838387E187698C504CFBA4CFA000AE73963576AA4119D967392BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	B0AE8911C62FE46331FC300C9D493BD79F3F69085DB98A56CA2777F4DD31AE1AAF7A811944EFB8F72E06F5965308F71125CB8C06CF9AAEC58F3BF4229D8125BD0E617DB4FC498E1D5610C4804AAE0028F32F0C8F31802B880FC4323E8E9C07F93914020BECBCE9FDA477966AA6900B
23	dfInput	00B0AE8911C62FE46331FC300C9D493BD79F3F69085DB98A56CA2777F4DD31AE1AAF7A811944EFB8F72E06F5965308F71125CB8C06CF9AAEC58F3BF4229D8125BD0E617DB4FC498E1D5610C4804AAE0028F32F0C8F31802B880FC4323E8E9C07F93914020BECBCE9FDA477966AA6900B
24	dfOutput	4B55CE228A3D0A8F01CC46520D6B844A4084EBC2F4BBA0DA9A543EECEEE3F54CB7E02DD3F4486A2E205593087F344A7636F2FA1654D100B3AE0C9F59F25EE1064A3FE356C562768CEB85E30512B906DA7B4B21337506312B917015FFE7C1676520DAADA369B4BE961AD8D28E983076
25	reseed_counter	1
26	output2	D761706653330AA76436FED3C9983D8110B9337DD859719C560187C4C2A7C2CD70CFB58592155AE4D907B242102E41EFEB42D73EF1A7900A2056DD266722E5299DB6FFB45B6A1DC12DFCA505A78D1CF49D1E3B949FF481C8E14BF6383127C1DCC94B4E8D699879F739F4A30DCEC7D563B419BCC6596CCB823790E02D638783A2B
27	H	6F66754954E691A275E1A966EA8C825F95AF12B2A1B3115DD969460D738B837B

		FD9CCDB70A12F6CA98041D60D7A4F7C78798528B3D525674A564E23253A24AAC
28	V	FC045734506CEEF233C8765EAAB4C021DFC454CB52752B31647BB6E1CC15A367675AAEED393823254E5C889ED23D41F6C333CF720AFD51EF1EF1FA671C62665907B413AD74BD6283AADCB4F8E8EA83010B47E4CCB97D274BA551A9161B5536E5F2413AECA8C81D3924329B4CE10B2E
29	reseed_counter	2

5.2.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
6	dfInput	00088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
7	dfOutput	6F8809E884E7142C7FB27A734CA23410157FD2188676A42B44D5D4150C6079E009B6CAC568B51312064C5F696EA61085D63D85A10A569B
8	V	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
9	C	6F8809E884E7142C7FB27A734CA23410157FD2188676A42B44D5D4150C6079E009B6CAC568B51312064C5F696EA61085D63D85A10A569B
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	964175AA23CCEF51D854889AAEABB58784664B3A2D6A2ED63ED877EE
13	V	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBD10D926BCF69BA40BCF096D6ADF78E5C5ADDB973E0ADD1AD5445C34BF
14	output1	A3728CF93C20B9DA29ACEC5C30240722031F513924F6EDBE5A97FAA09D7EB7F8C863132310D59624AE1CE1ECB6661A178565C83FF630A2ED
15	H	8EBCA84CC97FAB1E56D1B3798E9C473DA973792B41C8543E58146FE1
16	V	7816072AF43E0B81CCE09DCB127BD711EF13E2CEAD5F19A80D7191B4A22F83A02505F4EB43D5F7801B7962C0BDB679D27BAC993D7AFB3C

17	reseed_counter	2
18	V	7816072AF43E0B81CCE09DCB127BD711EF13E2CEAD5F19A80D7191B4A22F83A02505F4EB43D5F7801B7962C0BDB679D27BAC993D7AFB3C
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	017816072AF43E0B81CCE09DCB127BD711EF13E2CEAD5F19A80D7191B4A22F83A02505F4EB43D5F7801B7962C0BDB679D27BAC993D7AFB3C92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	E8D62AFEDC59FF1EF814C14273725F8F9E5DA5FDE9D679EDD9CF90F144E98B236920BD6818F131981D6073F961C83B90EAB01B9C7A6707
23	dfInput	00E8D62AFEDC59FF1EF814C14273725F8F9E5DA5FDE9D679EDD9CF90F144E98B236920BD6818F131981D6073F961C83B90EAB01B9C7A6707
24	dfOutput	3A523305DF9571B176A0F62538EAB458239925B96DD1DB311001277F580FEDE412A8458DA6B3BAE1C72249FA1A7F89A6C1933EACF994A0
25	reseed_counter	1
26	output2	E93BD0D85BF572225713D751DCF81A852F87944C877049536F6828E51B1E1FA62A9EA490600B7718895A2E641FB14BD1B04A9873B060916B
27	H	109F3768B216489BAF94934D0D0D4A191219C56CFF3D7A750FD8AABC
28	V	23285E04BBEF70D06EB5B767AC5D13E7C1F6CBB757A8551EE9D0B8813C30E1B992119EA554383986F1CCD705960D3236E9BDCF594CA664
29	reseed_counter	2

5.2.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
6	dfInput	00709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0

7	dfOutput	A7BEFCAA9C5CE75BE8DE729DFB1955DBA0001D0E2E1F155E879560897CAEA42F7DF963C35DDFB560C76988C1016FC09500E7ECC87038E6
8	V	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
9	C	A7BEFCAA9C5CE75BE8DE729DFB1955DBA0001D0E2E1F155E879560897CAEA42F7DF963C35DDFB560C76988C1016FC09500E7ECC87038E6
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	FADEB8700E75B36AA8A88224C44B79948A3045F84AB1C1BF918633DF12BBD42B
13	V	709B4FC7757F739BFD33872E36EF10823597958E0A9AC1319BC625F24421E3A6AADF87B5EEB6B802DA0B5FB5DE30C13E3C9C430C2D891B
14	output1	3C0E2ABFFDC9D947582E2220C0C46A8E62F21DD7EAC46668462A0F1B9127AEBAFEB18478AAD902E0BADBC662AE2600DC5598B319D1E1286DFAF7E60D6A9274EC
15	H	9C12524F05428CB9AC8088A57755FE206A22E97497284FD24D8573CB63DCDB09
16	V	185A4C7211DC5AF7E611F9CC3208665DD597B29C38B9D72C35ADD581035D4182A96190F0A2948DCDC45E5D0E07F05420C2F7FB387A9D0B
17	reseed_counter	2
18	V	185A4C7211DC5AF7E611F9CC3208665DD597B29C38B9D72C35ADD581035D4182A96190F0A2948DCDC45E5D0E07F05420C2F7FB387A9D0B
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	01185A4C7211DC5AF7E611F9CC3208665DD597B29C38B9D72C35ADD581035D4182A96190F0A2948DCDC45E5D0E07F05420C2F7FB387A9D0B92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	1FCA09F16CF8482078AF1D8C64EDBD2C80660563F8CCFBC6786E5FC36DC29CEE4332540D72D6E5D99DBB63EF4A1E8A70490D5D4691D1E9
23	dfInput	001FCA09F16CF8482078AF1D8C64EDBD2C80660563F8CCFBC6786E5FC36DC29CEE4332540D72D6E5D99DBB63EF4A1E8A70490D5D4691D1E9
24	dfOutput	E1E0F34D2D50A9B2E77749AE57054B075E0D96FDD29038961C7C81420A401BD6D0F5F061AB1E0BA00CE60204EEBD4B07CC3EECC606297C
25	reseed_counter	1
26	output2	1DD128C9F0AE50ECFCA77182F6EFEE04257CEC8F8BF257091C2A974CE1F029DA7E06EC321183ECA9D18C043DE5B04B2F91B32225635681C7E705ADC53D41748A
27	H	BCA7F399B374F3FC2DE4EBD69AEAED67B9A6BAC0D9F3ED7F17B828D0CA26CB4C

28	V	01AAFD3E9A48F1D36026673ABBF30833DE739C61CB5D35193CDE7AB8ECF6B4F2 F9141B0A08E25933515C26CE2CC9548FCD751AD6BEC6B2
29	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 LSH 기반 Hash_DRBG 참조 구현값을 제시한다.

5.3.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	44D27CF2997D8763F26BE77BA77A010263C9472DBB0CC9B88D8B04C619DCD7BC 1D0E0EEB026B8C786AE432984B9C21E1A039800068349727
	output2	DFDB71D8BEA4BE2D7B3B6B5E4B2844D19FDFFC63D749036D276BF88FF630F94C B601B8E2AE39F57A67CA94595AE9AE2A9A93D592C65ECF08

5.3.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	78C737EEB3F77BBA436AF67B4EEF4B6ADBBBD3476DA6C3B7869B13A66BB8C1E4 8F167C077956484C395437AE6951C5A86E7D8CC3F15EC47EBE8A83EEF41FC3FD
	output2	D2B03EF2732991BA8F48DC1CE4556FD9D9D92BD3CE7092B616011CC51B559905 9120E30B25BBC510BB1D1835873FD004216BF95A40DAF4DE35D848F0545428E8

5.3.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	ECD11A50E8D2AE8F4895BA8D794649D98087277855F346FA9F4C64308AD84BC8 ADA018BFAB283093C60BB6462484651D8834238EC6431BF61E4FC3A99364B604 7B5471A4F56DDAF9058CFA8E8CEC6406CCBCF22656688C7730EA15DF8BFC8D9C
	output2	766B4D770205946D2242BE51A80211820E1EC36257E1A0ADC522EAA9EF7E4E67 B76E43AF1EA3CA120DD5634FBCCD4401B92D869B221F8A17DAD60AA851C05B99 C4BAC887C516EF9882AE44B4370BD4790A42B2BDCDA96E11BD3D39DD45D2FC22

5.3.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	1864ADA72C1E9AA014E53C5D595481721FB144D37AFD2E8A6DB42A8FEED1E23E 658549C44BD7CDBA873096D8C9161EF04BBE60FA5973A91F5D37E265A883B85C 4DE2F6DED66E7DF3086FB56942B1A87D3E639C3C05E1D23FB8E49E6637964CC1 4988C06FDE3EDB80E12008BB442883A19F5403074E99D73254229C911C7FA39E
	output2	3B237E930DAF396036F784B87BCF0F11F0294589C67E3821B5F304C07BBF7717 F9119B5DA3924F2D584DDE141B4EEAB01FAFCF524E6A0DAB25435C8A4E0BBC0E 6831083414BD9544179790800B43A0B2746E8FFC3EA8AFBD58BCB0B0E6BC388B F2BABD83D4CF32E3452BAAD395D2543503666B2C57087263254671C9B09681E1

5.3.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	88C5A635D8163555BB46B9A4A270EE39D98B63EF11876D428DEF1CDDE7ABD622 FF45D217AAB879D706A20B6AF2FA512DC24672D759355BBC
	output2	95047CCFAE19DC107017DC6DA7E794693494AE650B113D154546E0E8568C1418 04C8E29CDDB9475DFE61DE973FF16F34D4190E4543CB0EF6

5.3.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	7CB3E15F79E259F568A705945BFD051938C1C1116FA06B6DFB1474298C871A4E 415C6CF83E756FFE37B7AC81459D27BE4C48C9DA87EE47CA5FC66C43C77BFF23
	output2	DA5592B46973585850B46B8951C3122EA9D60CA2ECE51FB5DF01E3FCCC9AA34F EC9D2709E46E69969D71927EBC6D0F8C92FCE8A5DF7DE83C3885CC299722E14C

5.4 시나리오 1-3 (개별화 문자열 사용, 추가 입력 미사용)

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

5.4.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	BB2332C211A3FBB3A4EBDF8F094CF25F724E8ACBA85B81AE4E7640CB7542B4D5 0FF11A7825591D2E96C55ACB9BDB6212DCFACEAD35C7B41B
	output2	B0572788E3D5DBFC1CC0AAA1328967D85F2EA6A7DAF68820FCB4B80801D0B5D4 F9715AEA95A8CF439E34D6EF82E355229B5DE9B6567B5EE5

5.4.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	C99F7BF366119FFB533E7D279D86DD58BE8C3ED17B989949EBE8BEF6AA9DF154 D0F604CF21BED1B543516A2A4E1331ABC1DFC370450F82D79A87947EB0CE90E4
	output2	55C8A63D7C647238F3569BFA4493F95E540D4BAB1BBA22045F65534675CE3D02 ECEA83D36470119A2CE275B19304BBBBAAE02370141D518D29A903ECFE166DE2

5.4.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	18A67BBE6502E3F726A1E75E4D3E51E8E6AF5281F4056E1658D1551A5C7E6016 132A9D189EB2D647BC8E9D88F8C19942E55518C9DC0D88EB1A8620A7C0A42F59 77726A4BD2E4D8EC9D316A52A2367B48D3E4BA2E6B50767143F386879AFF0D11
	output2	67B4AFBBEF9F213EF2A656F7045B5F636B85851A603B78FF0735DF7EDF445450 152BD90E908D94E4E7E753362D415392467731CE2199238A948F55A13F8586D4 A8A2244B16E12BD4E3A5980613ADCB8FD4CC36943601E3C2CBAD58932190BA64

5.4.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	E20C2079E350813860FCF2A9D82D88539A4197A6DBE34024B17FEB0E7E99C422 F9D3A2907D7698F1640038C73F92CB3A856E6CB4C8E8D1D5E2486B42B8886CBA 188C44338373823A6F7A3CB747EF1C2DF315367EB6879115F3A52B214BE8D045 FAFF0AC1AE3382C7F13F83C23E590B103E68086D94AC9148916D38A354357E31
	output2	15CFD44C7E7C2E3F6EDC7AC2681E3EBD7291C7A2BB3EB93384E32C480DFEBCB9 B8FE2C91EF16C5AB9533311B0E67F1B2D940C51FA91B5C80BC8B6C3399060FBE 22F130E175466BBE2E1993A642E506B1D1A80FA17BCD94203834EDA90B18F380 9B7AEAC8DB966027193C2D8207C3490F2812AC4FC0658726D4D50EE21DC2DEF2

5.4.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	273702F0DC2419513EE843B2D1801D71BDFC005489C7311B9BE621D4BBFD32C0 13C7A6FCE3631325B816F31AC40F9D70D716628BF1C260AE
	output2	8418DA37E65176B176FD943CE444F04A44A9518F9A16ADE55A8D6E2BC42418D1 868471CD3316C57956337FBDE66AB900801A702E2F4C8D4E

5.4.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	F5A094D269729B4E7CD56CE844C41B073332FB0ED76DDAC6FB87A4F9446AE7A3 7BEBB1974BC72F4AA1A103D6C095091CB837BA5814A00146250F52577FE77FCD
	output2	EC9D189DD0F3701D4CC2E7064A06C7473E6465958D985358D856DD0F74415B3B 772590A8D256C66C7232AB6575ACAAA87B01853A2549A680BDAF938AE16C9FC4

5.5 시나리오 1-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

5.5.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	BFA20B9B0E1438B005F0EC5F74CA30D689F725FDA7811BA70D15BB057328A69C 19FF43F399366F7C0AEE9B3F2E2EF4173D2D9030A28F94DE
	output2	71335DA77156A2167F168B41876F6EA359BF9D16E916ABECFDBF25FBD8FE2EF6 BA01D3FB60C87963A1AA8974715A5A1CAA32A2FFCA01C30C

5.5.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	DDB6AECE847B125179D9BF03730D6B5C5377F20F47518B5E414A7D316C1640EB FBE3DE2FC1C4F6023EA88BEAA2E818794854C63F291E9AA3CB2C4BB40DF1D115
	output2	B677D693585961645612 31A9C3DFB3CD00E594FE00C58A151B918FF0A87D6AB7 5DCD06B6CF8BBC1CEF040C4E41C090910FD1CB92C436A2A35FBC23602BE3EF99

5.5.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	7CFF622D16BF0082325230A4C0FCF4908E91381179D81972877B2963332E7382 5ADF1A8A846E72BA6804047764C4697A6422D9B7F901987B83A68A6E322BF662 82651069D88143A0B9FBCC850D60FED041F721BE57CC414350343130BD079D7C
	output2	0E10EDF7FEAD7921E23A4506AAD8CCC54C441007AB01CC4C031C70D39858A4E7 A21E9CD5521275B4A9CBB9C3293FE5E1A20D4DE9280AF3F5DF6AA8651E6C1981 62EDD4803FD30E38AFDC32105285D51119D9531D6ACF821DA11682AB595DC2BB

5.5.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	00A199A6E39B825FAAB85C79A1BC34629E7C9F4A298B887F9C9BBA82A5FA480D B628F6F2A64A5C198B872115494A23B54F27930D622C1BF713ED717E23930D63 9A7EB954FE45F12014B4808AA5E890B6D2CBC8C8805B140A5197328134B3A151 1AA6A7DD04819B56025DCB0211D6F51691568A535531 0835D78055D67FDF2E27
	output2	1B69F202A60D91CA154D1D9F7DE4810404C2ABC9628CE8AA7F18E63059D33BEB 082F1F90AEB75505977EBB79CAF3A99CD4014D34845FE432BDF6D90DB1659A57 47B10672EA03EFC75AD82CE23747FAF426A95E41748997CE3D99A3CC4B2B1AAE 69B6A3657EB8D4C9EC1823BC1BCE9CA0E252BC9ECA32F2A914A7BDEEE108269E

5.5.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	131A1DF4992CD45BFBA27F8627C40344F61CA5011278C70514E91A4203C629986F0C9D2E3BBAB0844AA052798CCEE4694D0DA57DF53C202C
	output2	A441AB3A393FCD465D9C1DAD07063864B3BB5328706CE87050D2BE6FDD1A23F74A08DC0EAAF11F27D603CE4CBA9A88EF5A3F9B6DD7F88354

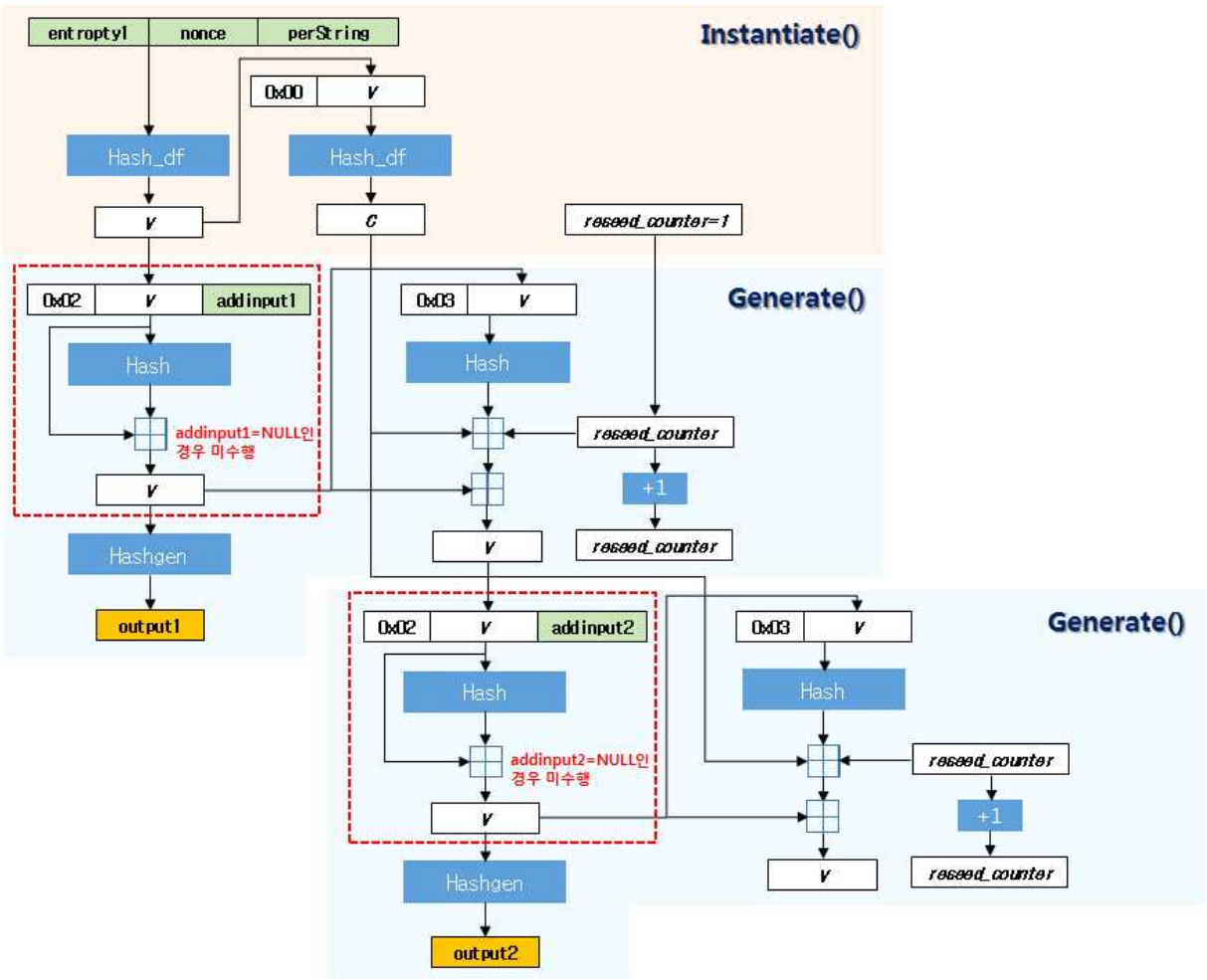
5.5.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	62E175D7D88F44FA1DF89179B86173976C2FB708A8012EACB0F23901AFB7BC6BA3EA847E9691129112C327F8984D5FC999D68299A09D57D0D56F0D095D6DC932
	output2	5C1D11B84AB5E69AF1DBDEECB465006DE5023116E71CE25522FA8A0681D63FAA03743F99143E29385A7CE8955F083FE883AD57C00D87E58381F6677FC945414C

6 시나리오 2 (예측내성을 지원하지 않고 갱신주기를 2로 설정)

6.1 개요

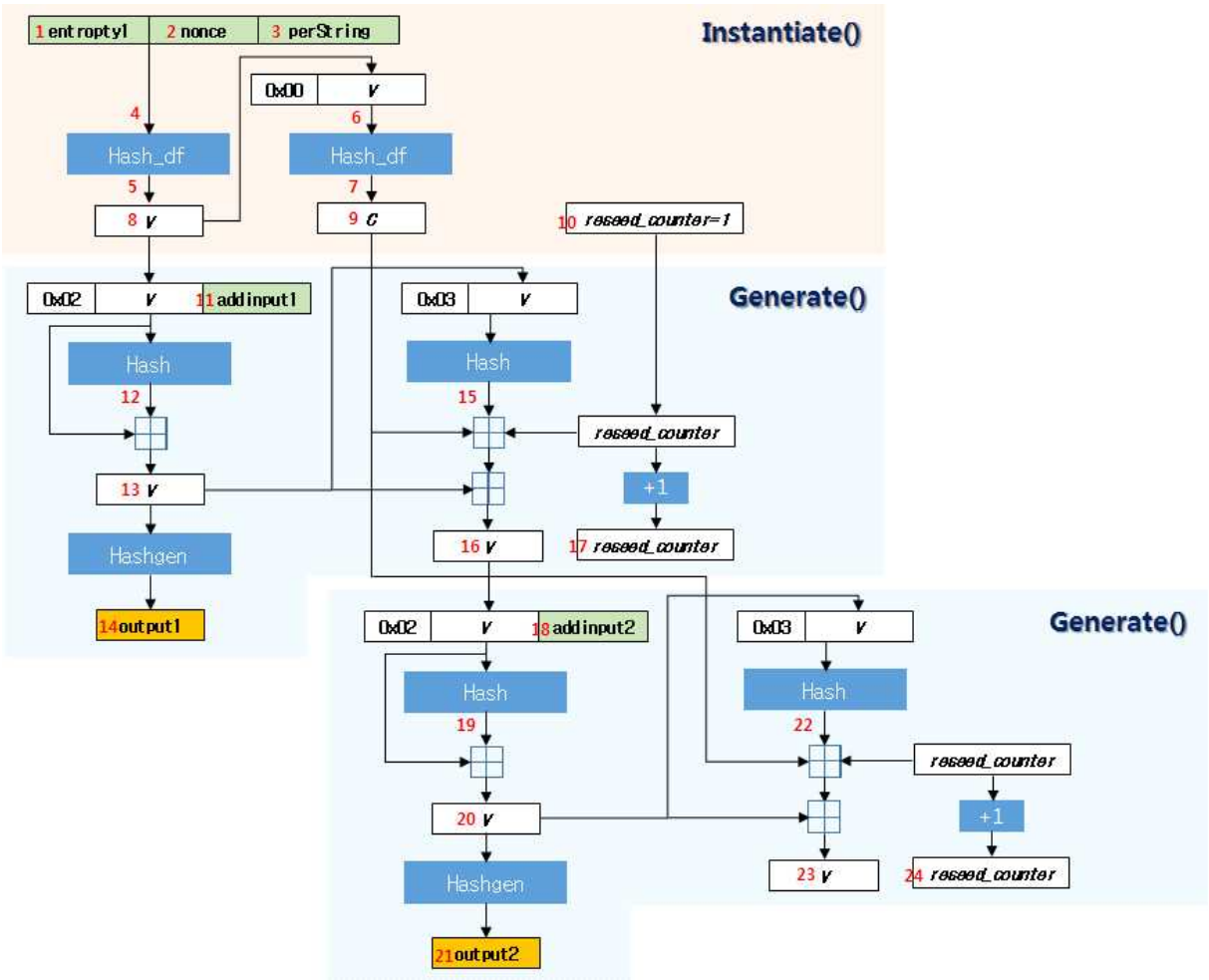
시나리오 2는 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 2로 설정할 경우의 LSH 기반 Hash_DRBG 참조 구현값을 제시한다. (그림 6-1)은 시나리오 1에 따른 Hash_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 6-1) 예측내성을 지원하지 않고 상태갱신 주기가 2인 Hash_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 LSH 기반 Hash_DRBG 참조 구현값을 제시한다.



(그림 6-2) 단계별 참조 구현값 위치

6.2.1 LSH-224 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405

5	dfOutput	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E663 05DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
6	dfInput	00023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E6 6305DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
7	dfOutput	4126A8395AD8D221D183027BC02A1A773B8AF98F0AD66D946F799391F0134944 A603AA7D8DCFF7726EA2A91E157E02A6F92B10031F9486
8	V	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E663 05DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
9	C	4126A8395AD8D221D183027BC02A1A773B8AF98F0AD66D946F799391F0134944 A603AA7D8DCFF7726EA2A91E157E02A6F92B10031F9486
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	FA920888ED46415195311AD5C1417455285E63B60187F10ECC87ED30
13	V	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7E1B1EBD6F50 4C1DF73F869EFDEBA0BA52301DF7E61784B8BCB86C1ACD
14	output1	3C8436BBDA0084585D66B05F5599316A05FF0C273F230C8EDA258C981A42744D DA45FDC8067AD4B514712C6187FE6B4FE783B192B3A99A07
15	H	8FE291EF003FD9043747D16D4879778F55C0D183651B6BB48CE036D0
16	V	43626552076E1AEFC25603CC6E016BFA69FBE5159CDDD23C7047123CF162A795 31FAA5F45C4062A688D48AA3F4476C23994F81486BE624
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	6654E233905ED57A4F9367A719F43C6CDF8D3F334DA86109808C2A7F
20	V	43626552076E1AEFC25603CC6E016BFA69FBE5159CDDD23C704712A34644DB25 90D02043EFA809C07D10F78381869F7141B08AC8F810A3
21	output2	AD01878588665EF0BAD24CC5286D4E00A7DF0C6AFC00D9710403D09464343659 B93689F88C3253E87717805FCD5C78E04CA74C2054EB0E06
22	H	8B37D21CFF616B856DA98F7BD99FC5B36061D77CB889DA8E6422CB40
23	V	84890D8B6246ED1193D906482E2B8671A586DEA4A7B43FD0DFC0A6C06E2A4169 983F502F27077D0C8B795401F8DC1ED0C4B629303A706B
24	reseed_counter	3

6.2.2 LSH-256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	df0utput	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AE EAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
6	dfInput	006B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39 AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
7	df0utput	9D6B66A8636E1B65248705B2DD0CFDA1A0BB594275022EB49A8B35B57919FCA9 CCD43D316D95B300340815C46DD47E9DFF600C75631A61
8	V	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AE EAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
9	C	9D6B66A8636E1B65248705B2DD0CFDA1A0BB594275022EB49A8B35B57919FCA9 CCD43D316D95B300340815C46DD47E9DFF600C75631A61
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	0011F71DA9E5159A7378EBC73F9475CDE53EE9F013255385CC000D80D571D5FF
13	V	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CE1A0BA970CC4D422 63E1E3E0F28EEE19164744AF3DD9A3CFD8A238D102CDCA
14	output1	3BE9C1A3C3DC9F57C57ACAF36A54F6F9C3A28CF6D7848540D88A9DC31461A927 9F6B45AEAECF9AD81E43B1EC674ABC0EE57347E4392D270E3E0578A99252F41E
15	H	0365C0CCFD5E91CFAD573FD606E7BA621C8BBA4016B3AECED4CD4CD455E8B07A
16	V	0885ADC3CD32E49010622736EEF25199097E6C3AAE6775D4E1ECBD49E470A079 87F5F71947DF0335D6099A8A5F5CF142A54F199C4E98A6
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	B46E6988103018E6D8BAFB1F49D846D07FB064AE9C738712368261CEFFD0AE5A
20	V	0885ADC3CD32E49010622736EEF25199097E6C3AAE6776895056455A14898752 42F116632025D3B5866E4926D2E4037927B0E89C1F4700
21	output2	1AB184213F748634EDF598BD44C6B1549653D5202BAAACC0539982C8C5AB300A A748E4B4AD734EDA70FBE55E363342E14D5A4D49CC7ADB657D7500BFE96B95EC
22	H	0EAA12AFA9A10E5F852C097FBE6C662F33DF3D4361DBCC948F28D762259C306C
23	V	A5F1146C30A0FFF534E92CE9CBFF4F3AAA39C57D2369A54C94F42AB92EB1E381 3BCED352FA21B5E999B3A24D1C8516A64FE857371E91CF

24	reseed_counter	3

6.2.3 LSH-384 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C2 9264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0A EC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8AC BA62997B7BEA6A975D6D256DDCCFF1
6	dfInput	00E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29 C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F 0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8 ACBA62997B7BEA6A975D6D256DDCCFF1
7	dfOutput	B5E5365A977CA11A5AE9D0EE37A325A920316E2C37726E6EE98A4ACA53ED64B9 19A69356D639A679D0877E2467939B429676EC676A303F1018A965B21C38672A E85099122EE5826454764D629E1318948BA67ADE9DB7E85D36D4331CDAF990A7 E3FADA75E59F144F9D643265ADF07D
8	V	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C2 9264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0A EC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8AC BA62997B7BEA6A975D6D256DDCCFF1
9	C	B5E5365A977CA11A5AE9D0EE37A325A920316E2C37726E6EE98A4ACA53ED64B9 19A69356D639A679D0877E2467939B429676EC676A303F1018A965B21C38672A E85099122EE5826454764D629E1318948BA67ADE9DB7E85D36D4331CDAF990A7 E3FADA75E59F144F9D643265ADF07D
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	E8D69C9136CE8A49675FD83A229217152948B077AE40C6251A878F2C61EC3089 ABDE71FCDF0C01C6061F8133D7A42D1D
13	V	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C2 9264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575FF3 C2B70C20174137667DC17B865FA557C0E3B64372CD2C67706AB7C73EF2875258 98D4965A87EC309D7CEE594580FD0E

14	output1	1D8B23825439377ACB4E7B6C5EC4F573C039BCC07522916DB7C295AF6B9A136D800F23969C3CB2D01D0D780A7A1043659A843067DCD8D93334222E5CEBD1B794336C8D3AA99B3572002E7F7F17AA87B9D9EF8D64B693EF0E2F8B21582070388E
15	H	6B50360DD2EF6C409000299F771C68B462B8BE9ACC4849DEF46612D47674CEAA4B7787A90D332CD5070CD8084C5366FB
16	V	9A6348064E378B88CB8F56DB4AAC16B8C00791317B6A35EEA8C4BF325AC98E7BAC0B5D17D3C95863B3B3012BFA8E6CF594FF4A6BD334068654E451D0FB8FC789FB3DB3053592FA5AD26168601A2124B8281B591DB32E2EC2079ECED2424F8D4BF45719DDA0B819F4272A93F7825487
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	29068F2F2BC53220E718FBD1374CA4A13F00C7CA96C24B93828503EBC090E81039DBC2ED3DA11E173A93E8059FA5244A
20	V	9A6348064E378B88CB8F56DB4AAC16B8C00791317B6A35EEA8C4BF325AC98E7BAC0B5D17D3C95863B3B3012BFA8E6CF594FF4A6BD334068654E451D0FB8FC7B301CCE230FAC51B41EB5D399766C5C5F728E323B47579C2448CA2BA92D3379D85D01A071B41D6312EBB1299972778D1
21	output2	525F6976BF63645DA42B6765287BD30BEB6BC18091A7189AFDF7DB657CDA195DA2E873EB71607FBAA1E801A6972C439A1B6BE86076194C1487AB0A80FBEF3AF68734611AF6141F5BD1BC86084AACD880D62D3E01E777FF757431857219AD51E7
22	H	618B539B2D29385F31C85500C329F5634D032B395801F5CF58A9B08427E8CDD6D0CF5509B4D1693F9CA81AE26B7484F1
23	V	50487E60E5B42CA3267927C9824F3C61E038FF5DB2DCA45D924F09FCAEB6F334C5B1F06EAA02FEDD843A7F50622208382B7636D33D6445966D8DB78317C82F3F7571167052E2FCD8082887BD2ECE41D8B7B4D7EB152779FA6D2771D796FF04FE8369EB45F8DE851B0091AE6849EE41
24	reseed_counter	3

6.2.4 LSH-512 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C

		92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B
6	dfInput	00ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B
7	dfOutput	BC1648BB27119BABE1D09A426BBC66DA6FA54C1C432AAB80F46C0645492777138570503 6AD4986F0FB0FC73FB1C2F7696256EE93B213D25DDD556D0DEE90E0C5EB74B3DFA65C99FDB60A367577CC06FFA7AAFB496818FF2462F12028B691AEFE8DAB3BA702FA2ABE9C7D5FDE6A1F2E
8	V	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B
9	C	BC1648BB27119BABE1D09A426BBC66DA6FA54C1C432AAB80F46C0645492777138570503 6AD4986F0FB0FC73FB1C2F7696256EE93B213D25DDD556D0DEE90E0C5EB74B3DFA65C99FDB60A367577CC06FFA7AAFB496818FF2462F12028B691AEFE8DAB3BA702FA2ABE9C7D5FDE6A1F2E
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	4E8B7E1E3B2C9948770C7B4C3D980F2F7958F585DDC940CAB3A6C9763308B4C474A6D94B1A7B6A68789455BC47B8454 79DA7A5B30C4B6C29264F2ECEB58505AD
13	V	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389305D0736235A6E579F9194228C294C78B9D5EBEA8230EB6376D2EF537642D7C612F2D5E1A37751F2213C8A6ACC98E29DF6FF45744A5AD6D012541A20F4E6BEA108
14	output1	6B51E02F8C250DE36439915EC8A8A80996A8B21ADF45DB32F7BBF86942D16F824F2E8C0F6F1B5D9C3511F3262D69547585D5240036E4EEC041986B41879A837FD5717E9CCEDE03DFD2F6092165DBF3E550250C3918E0B7B4DF8258E963DF28AD28828255649019DBBE52F1FC82862D33FE431A51951CFD618B730EFC88C39CE2
15	H	90F0F08FDC65536E4E17C38D1B9FEAE4DAF115155153348F51716B7353E764B7389B41FCC9C142D7D74B222BB4FF955ED1E72D73FE311CFC50A0CC4F4C74D63C
16	V	A97B48A3E7FCB4DAF808659C3E69AB4BF83A7B3B01851AB9E8E1BF9F64B8E5C0F8437B048C78ADE49F64B740154C28575A7DA1CA85BEE03D893B8652DAF47F76C8744B61E4F4A02216C9200C36F6D12B18CE9B8A7B4DF838387E187698C504CFBA4CFA000AE73963576AA4119D9673
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	8BC360EF2771B65E6B97A6CFC57A00994409272DCA8B86476FC3EA4F21324029

		BF6C1F5C0C0CE021B9608616068AFF715AC7798588F952ADC3FF484606297410
20	V	A97B48A3E7FCB4DAF808659C3E69AB4BF83A7B3B01851AB9E8E1BF9F64B8E5C0 F8437B048C78ADE49F64B740154C28E31DDE90F1F7753EA920E2561854F518BA D19B792C707AE791DAB36F2D6936FAEA84EDF796882E19F199042E7D23C4762A 81C67F890439E72756B2EA17C70A83
21	output2	8CD927608CBE20D3B7E07FD7E0EE8966FA61C20D6BEAF93B106AB969AF97A403 04C6EEE4BD220E52A4876288DED2F70141B352622196A0535201B05234A03CFD CADEFA7A22E40A88FF6E7D1A2556F00F56CE49375923AC741131A46CCF876FA0 09503B9FFA33DEF36EC12A22C6E282939B28DEF0023107637C77FB05DEA0CCA7
22	H	FCD9A05210D97199AEB88934FB2E0E61479F799C61E57DEF577426CCFAF4AE96 E6320E6D0962237BE4B5F703145527BBE1A2AB06F1A3C30F275B8129797B648A
23	V	6591915F0F0E5086D9D8FFDEAA26122667DFC75744AFC63ADD4DC5E4ADE05CD4 7DB3CB3B39C234D59A747E7FC70F214959D5D19682FAAAB5B6C0F82171945AC8 5C89C96DFC5570E704E4729DD5B198D05EA75FE9526A94FAB1EC51BA2F7DE10A B21CC221AAF7210D4EB1736FAC8E3D
24	reseed_counter	3

6.2.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	df0utput	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2 CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
6	dfInput	00088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112 D2CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
7	df0utput	6F8809E884E7142C7FB27A734CA23410157FD2188676A42B44D5D4150C6079E0 09B6CAC568B51312064C5F696EA61085D63D85A10A569B
8	V	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2 CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
9	C	6F8809E884E7142C7FB27A734CA23410157FD2188676A42B44D5D4150C6079E0 09B6CAC568B51312064C5F696EA61085D63D85A10A569B
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951

12	w	964175AA23CCEF51D854889AAEABB58784664B3A2D6A2ED63ED877EE
13	V	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBD10D926BCF69BA40BCF096D6ADF78E5C5ADDB973E0ADD1AD5445C34BF
14	output1	A3728CF93C20B9DA29ACEC5C30240722031F513924F6EDBE5A97FAA09D7EB7F8C863132310D59624AE1CE1ECB6661A178565C83FF630A2ED
15	H	8EBCA84CC97FAB1E56D1B3798E9C473DA973792B41C8543E58146FE1
16	V	7816072AF43E0B81CCE09DCB127BD711EF13E2CEAD5F19A80D7191B4A22F83A02505F4EB43D5F7801B7962C0BDB679D27BAC993D7AFB3C
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	C793673341D83249A721CBFAFAC247A62863856BEC380FDC26C39576
20	V	7816072AF43E0B81CCE09DCB127BD711EF13E2CEAD5F19A80D71927C3596B6E1FD383E9265A1F27ADDC108E9213BE5BEB3BC75643E90B2
21	output2	2FE15FACA62D94D46635F4E7531A75FB0D164BE40F8560B711C740A994793FBB5A27F3DD732DEDE580442FB6CA86127EF63EF62D83965E2E
22	H	9FCC15870EB872D08D1DEC9E978D196E0948EC067967CEE7858919EB
23	V	E79E111379251FAE4C93183E5F1E0B220493B4E733D5BDD3524767310E0CB7D0BF61D9E4EC43A4247126D65BD8CDFCBDF1C8E28AD2013A
24	reseed_counter	3

6.2.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	df0utput	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
6	dfInput	00709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
7	df0utput	A7BEFCAA9C5CE75BE8DE729DFB1955DBA0001D0E2E1F155E879560897CAEA42F7DF963C35DDFB560C76988C1016FC09500E7ECC87038E6
8	V	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE

		025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
9	C	A7BEFCAA9C5CE75BE8DE729DFB1955DBA0001D0E2E1F155E879560897CAEA42F 7DF963C35DDFB560C76988C1016FC09500E7ECC87038E6
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	FADEB8700E75B36AA8A88224C44B79948A3045F84AB1C1BF918633DF12BBD42B
13	V	709B4FC7757F739BFD33872E36EF10823597958E0A9AC1319BC625F24421E3A6 AADF87B5EEB6B802DA0B5FB5DE30C13E3C9C430C2D891B
14	output1	3C0E2ABFFDC9D947582E2220C0C46A8E62F21DD7EAC46668462A0F1B9127AEBA FEB18478AAD902E0BADBC662AE2600DC5598B319D1E1286DFAF7E60D6A9274EC
15	H	9C12524F05428CB9AC8088A57755FE206A22E97497284FD24D8573CB63DCDB09
16	V	185A4C7211DC5AF7E611F9CC3208665DD597B29C38B9D72C35ADD581035D4182 A96190F0A2948DCDC45E5D0E07F05420C2F7FB387A9D0B
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	1B7038F787008053BC79F8E81B869633ABD965D84C4643CA96B8DE4CCE543A96
20	V	185A4C7211DC5AF7E611F9CC3208665DD597B29C38B9D747A5E6CD0803DD953F 235A790C292AC1799DC4355A4E341EB77BD64806CED7A1
21	output2	F1FEA82A3E5E2E63CD31750542F23D4E1E86614DE7DAE5F3EEEB4D4B47FC9658 190A1A1EE838433191612855BA626C9CB1A0C98DC65DF50E08764872EADCCEED
22	H	1C2C7F7C5DD256A730F6A14B84BCA8B65725221667951D21D2D8347347CA693C
23	V	C019491CAE394253CEF06C6A2D21BC397597CFAA66D8ECC259FBA9EF52E2E09F 97F5285443B32D318A4FD482E4C1011F54F2A8170979C5
24	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 LSH 기반 Hash_DRBG 참조 구현값을 제시한다.

6.3.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	44D27CF2997D8763F26BE77BA77A010263C9472DBB0CC9B88D8B04C619DCD7BC 1D0E0EEB026B8C786AE432984B9C21E1A039800068349727
	output2	24E58D83710EEA97E4CDFD3032D528935CC3CEAFA36AEF45A92BE11391E121AB B67A7ED753396E926ED4E066A4E33AEC4A03DBE4238CA016

6.3.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	78C737EEB3F77BBA436AF67B4EEF4B6ADBBBD3476DA6C3B7869B13A66BB8C1E4 8F167C077956484C395437AE6951C5A86E7D8CC3F15EC47EBE8A83EEF41FC3FD
	output2	6B90BA9243103385950D41C4A55761310778ACF38BC38341FBC154AB4C12F601 3D36C7F760DB10D374ADE1A31287E5EDEA18EB86240D214A6D82834149E3747F

6.3.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	ECD11A50E8D2AE8F4895BA8D794649D98087277855F346FA9F4C64308AD84BC8 ADA018BFAB283093C60BB6462484651D8834238EC6431BF61E4FC3A99364B604 7B5471A4F56DDAF9058CFA8E8CEC6406CCBCF22656688C7730EA15DF8BFC8D9C
	output2	5E0D7B84A9F9F61B910F36A1D653CEE2010DDA7ECCFA50D80783824607B153EF B03240AFF463F7B9C9F6256DF3C7E8AB18BE7BE8C08C4BD88C5B9B930BCF1CCE E887303570D3847A91495B95BF714315A09A82FF23551794FC41AE308F0297C8

6.3.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	1864ADA72C1E9AA014E53C5D595481721FB144D37AFD2E8A6DB42A8FEED1E23E 658549C44BD7CDBA873096D8C9161EF04BBE60FA5973A91F5D37E265A883B85C 4DE2F6DED66E7DF3086FB56942B1A87D3E639C3C05E1D23FB8E49E6637964CC1 4988C06FDE3EDB80E12008BB442883A19F5403074E99D73254229C911C7FA39E
	output2	5EDA01D4FC7A0656FAD4BBCAB1237D737FE51CA89FAB171AD2C468A486D17741 16B0B13ABC560BA24340EAF44A40E9AA6FA7D9AF1DAA9FA64ADC74DBB6818615 B8094DE8B6811723BDD989AB764BD0819B9BFE867D004DAA0D57DED98984F3F8 3E55E2F122E8A16BBA06F5CEE7035458977AD5617EC280DAB4A94041B1A14F05

6.3.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	88C5A635D8163555BB46B9A4A270EE39D98B63EF11876D428DEF1CDDE7ABD622 FF45D217AAB879D706A20B6AF2FA512DC24672D759355BBC
	output2	5668084F34340442637263375B91224A04A8152A18B92FC9D034CB27E7AF0339C B818842D6946585920913784895 3D3F14BCADA40B73D5B4C

6.3.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	7CB3E15F79E259F568A705945BFD051938C1C1116FA06B6DFB1474298C871A4E 415C6CF83E756FFE37B7AC81459D27BE4C48C9DA87EE47CA5FC66C43C77BFF23
	output2	19C32DE203A8C94DA838F0B99C982D71DE77E05CBE387AAC37786DD690AC8E39 C1EDBAB01EFA99BA8CEAE482812BB36F9E13EDC12C089BF599ACABA4C309321C

6.4 시나리오 2-3 (개별화 문자열 사용, 추가 입력 미사용)

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

6.4.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	BB2332C211A3FBB3A4EBDF8F094CF25F724E8ACBA85B81AE4E7640CB7542B4D5 0FF11A7825591D2E96C55ACB9BDB6212DCFACEAD35C7B41B
	output2	1D52D7A79794588C87484A6CE769D453DED0DAFE809AEDBFB16BEC8AF064F957 B6C5275E8094DDA05B66DC0E61ED0D4D142729F2ACFDDB2D

6.4.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	C99F7BF366119FFB533E7D279D86DD58BE8C3ED17B989949EBE8BEF6AA9DF154 D0F604CF21BED1B543516A2A4E1331ABC1DFC370450F82D79A87947EB0CE90E4
	output2	2971B5592F724897A258FA47B02C8F0B86CA718F63367A70AA223F56BCCC95E5 99118E58D67366C1F53A5B0428FC40931871DFE5395BC8CC1AB96E8B593AA2FA

6.4.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	18A67BBE6502E3F726A1E75E4D3E51E8E6AF5281F4056E1658D1551A5C7E6016 132A9D189EB2D647BC8E9D88F8C19942E55518C9DC0D88EB1A8620A7C0A42F59 77726A4BD2E4D8EC9D316A52A2367B48D3E4BA2E6B50767143F386879AFF0D11
	output2	544AEA9C502BD77848196E21839B8BF04AF040BE0938465CC86828324F4B0EE2 3DCD5C1932CA2D21E3166175BE3B6C6E4BB22D079154B81D1722E4F5A7DAC9DD 3D6C4CCBA2B77B523BAB6134089B88F6A12D7E3A2466780800120E26144F304C

6.4.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	E20C2079E350813860FCF2A9D82D88539A4197A6DBE34024B17FEB0E7E99C422 F9D3A2907D7698F1640038C73F92CB3A856E6CB4C8E8D1D5E2486B42B8886CBA 188C44338373823A6F7A3CB747EF1C2DF315367EB6879115F3A52B214BE8D045 FAFF0AC1AE3382C7F13F83C23E590B103E68086D94AC9148916D38A354357E31
	output2	68BED7D313AEBE5645B5F8A901354F412B6CF8855F19687A3F0EB646FF2DD0F5 4953385F64899983B477B07C707F01962EAF0D238BC383FBEEEF0AF9FC38582D D08BB60D7CC82896FA9302A239EEB8D686DD9C96D3A3C804A5AF3D0A7D03F42C 9DE949C08210D3029618E3D437A318D0ACD847931F459E977CF86A6E3F2F1E8C

6.4.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	273702F0DC2419513EE843B2D1801D71BDFC005489C7311B9BE621D4BBFD32C013C7A6FCE3631325B816F31AC40F9D70D716628BF1C260AE
	output2	E259D4EB0F9AFC3E2714578FECF6E3E82D5142502C5CE1FE4CAB367BC8DBD93C8C997850F258882FA471ECCD74C09A1C5BA58282EB662E99

6.4.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	F5A094D269729B4E7CD56CE844C41B073332FB0ED76DDAC6FB87A4F9446AE7A37BEBB1974BC72F4AA1A103D6C095091CB837BA5814A00146250F52577FE77FCD
	output2	113E98C55F4E5ACCC2623FA5238918AB6FB387469758FDA874BE9C2707DCD01098E3CA35E9C50F9D5D8211A07FE63A5CFAD6219F23F1439F8CF0A2F62560893E

6.5 시나리오 2-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

6.5.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	BFA20B9B0E1438B005F0EC5F74CA30D689F725FDA7811BA70D15BB057328A69C19FF43F399366F7C0AEE9B3F2E2EF4173D2D9030A28F94DE
	output2	16F6BC3A5D988974A359A4BD9C86DE3343F1715A767AE4A715A9766B2F2DB29F7B408B164F10F95547601857ED401F4CBFDD2010C3AACD03

6.5.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	DDB6AECE847B125179D9BF03730D6B5C5377F20F47518B5E414A7D316C1640EBFBE3DE2FC1C4F6023EA88BEAA2E818794854C63F291E9AA3CB2C4BB40DF1D115
	output2	BB46A3A85565B525B41ECD62CE41AF537F9E65AB247CC2451D48FBAF1FDC76B175D1AC5CD77004EDA431718439EEEDDE79A4D522152A7B7616A268FE00C8BCC4

6.5.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	7CFF622D16BF0082325230A4C0FCF4908E91381179D81972877B2963332E738225ADF1A8A846E72BA6804047764C4697A6422D9B7F901987B83A68A6E322BF66282651069D88143A0B9FBCC850D60FED041F721BE57CC414350343130BD079D7C
	output2	7FBC60EA0DC4B0AFAF27868593924F25FB6C7594943DC2C2B0F062A208675BC19F7516498EE1CE6860A7871E7FC0E50A95B211AF478B293D47E88170FC8DF501C08AD263CBE53D13476EFDC6B186FF428379ED6ADFD6ABE9AE92D6D379F6E4F0

6.5.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	00A199A6E39B825FAAB85C79A1BC34629E7C9F4A298B887F9C9BBA82A5FA480DB628F6F2A64A5C198B872115494A23B54F27930D622C1BF713ED717E23930D639A7EB954FE45F12014B4808AA5E890B6D2CBC8C8805B140A5197328134B3A1511AA6A7DD04819B56025DCB0211D6F51691568A53553 10835D78055D67FDF2E27
	output2	3D300B98AE54F3AAD943E8E840F3C1C72F9F40C031E81CB9BC184610BCA3EE313A9EE96CB5968E91B99E2379E643182263 5C9A609138F42FAA5DCBC406D297C959B412B22226A45990FE5D6A4562F13D958D97727AA124F3F3EB6C73B8EB13684043596E85F3269E34AED6B1C6E0A523911B6BB552D64E0AAC33110322B0885D

6.5.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	131A1DF4992CD45BFBA27F8627C40344F61CA5011278C70514E91A4203C629986F0C9D2E3BBAB0844AA052798CCEE4694D0DA57DF53C202C
	output2	E186A1F945445628A14D6EDFEB9A9A5BDDDDA6D12E8239B565969F0BB816506AAFF129E9503D4DCF431D9E950DA9C97E796EAB8AF77C4751

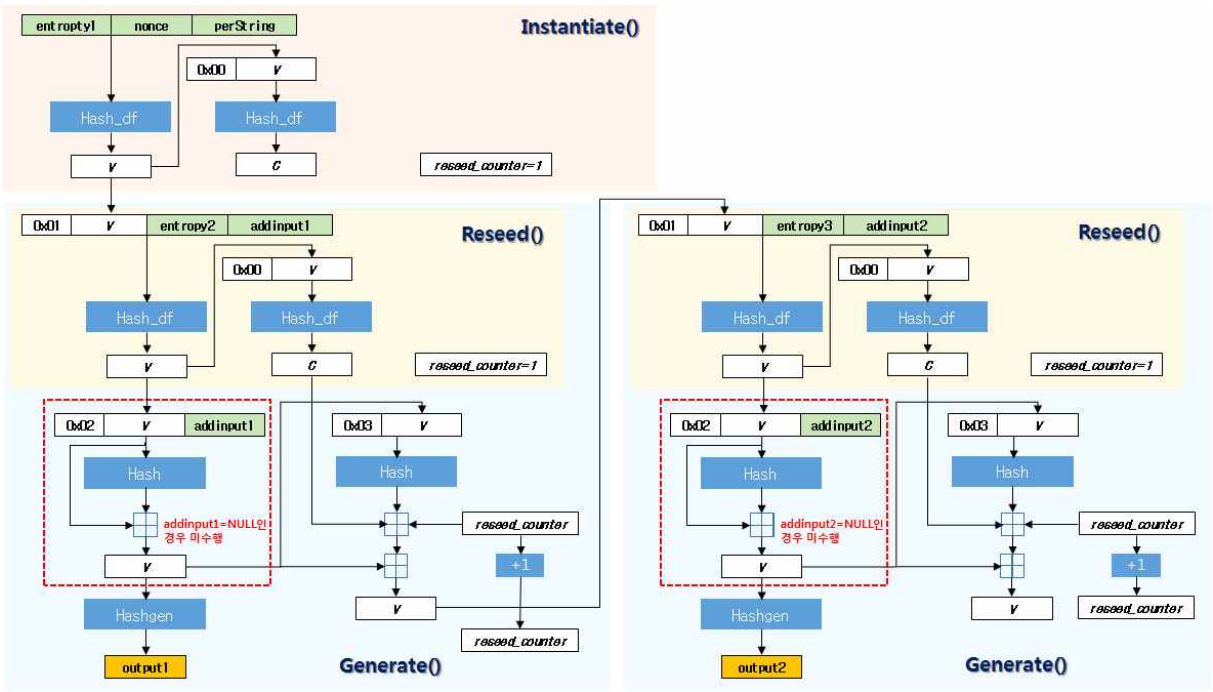
6.5.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	62E175D7D88F44FA1DF89179B86173976C2FB708A8012EACB0F23901AFB7BC6BA3EA847E9691129112C327F8984D5FC999D68299A09D57D0D56F0D095D6DC932
	output2	353547D7B905938EE5C293964F2E610893682C18DFE104122B9E38D194025D8ADF1A6F387CFDE06117AAC8D785C17E7170FAAFE170567C03DDB1293D38465317

7 시나리오 3 (예측내성 항상 지원)

7.1 개요

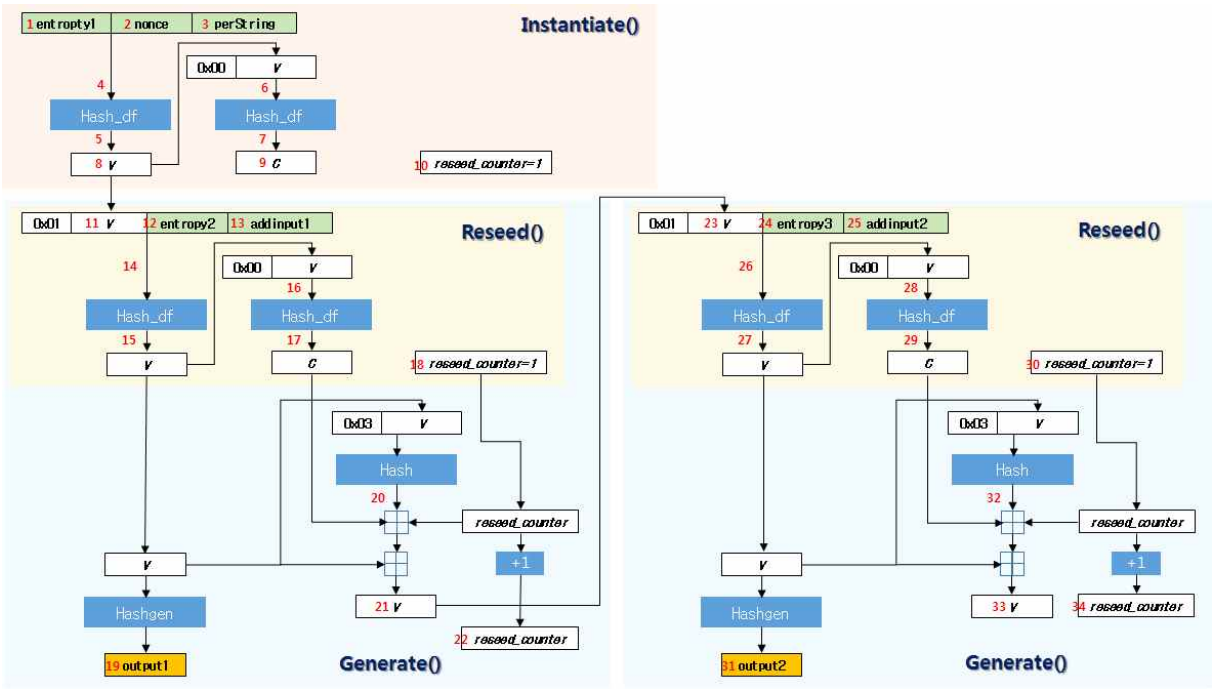
시나리오 3은 예측내성을 항상 지원하는 경우의 LSH 기반 Hash_DRBG 참조 구현값을 제시한다. (그림 7-1)은 시나리오 3에 따른 Hash_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 7-1) 예측내성을 지원하는 Hash_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 LSH 기반 Hash_DRBG 참조 구현값을 제시한다.



(그림 7-2) 단계별 참조 구현값 위치

7.2.1 LSH-224 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E663 05DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
6	dfInput	00023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E6 6305DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
7	dfOutput	4126A8395AD8D221D183027BC02A1A773B8AF98F0AD66D946F799391F0134944 A603AA7D8DCFF7726EA2A91E157E02A6F92B10031F9486
8	V	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E663 05DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D

9	C	4126A8395AD8D221D183027BC02A1A773B8AF98F0AD66D946F799391F0134944A603AA7D8DCFF7726EA2A91E157E02A6F92B10031F9486
10	reseed_counter	1
11	V	023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E66305DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01023BBD18AC9548CDF0D30150ADD751832E70EB86920764A800CD7D208CB4E66305DCA5AA5584282A5F45FD07BF943015FCC7ADEBE42D9D92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	dfOutput	17E21F096689BB6677F799E506762B301BB9FDE066C3835CCEA79E1D3A821F9F6A46AFBE97111A38FB2391BBFE989D6E41238B844717D4
16	dfInput	0017E21F096689BB6677F799E506762B301BB9FDE066C3835CCEA79E1D3A821F9F6A46AFBE97111A38FB2391BBFE989D6E41238B844717D4
17	dfOutput	4A59F81A32202220F8B361120B197B04D583B29718DE8A25123BB1CB20D38B96E3D5E252A5455BADFD367EA629BA73F557AF66CE4FE77C
18	reseed_counter	1
19	output1	5526F0705308A574CE313F5CDAB8C8AA0ABCDFB2D6B87469F049DCB059B5037E4877258C8A4ABE2DDD1D51BAB2D53E63913B2FCABC3C4A89
20	H	EF28856851CFB1342C825E2F75615DC7556C0B175790BEA98174FACA
21	V	623C172398A9DD8770AAFAF7118FA634F13DB0777FA20D81E0E350D783DB13881DCDC63DBEB4A55C59B7D7B7945E28BB29919BD40BFA1B
22	reseed_counter	2
23	V	623C172398A9DD8770AAFAF7118FA634F13DB0777FA20D81E0E350D783DB13881DCDC63DBEB4A55C59B7D7B7945E28BB29919BD40BFA1B
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01623C172398A9DD8770AAFAF7118FA634F13DB0777FA20D81E0E350D783DB13881DCDC63DBEB4A55C59B7D7B7945E28BB29919BD40BFA1BF148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	dfOutput	A13D0A8563DA7EED1BFFA9DE862B4149BF8658EA8DA5034DE52D88E04875EC57F85B55C10DD5B0563BFECE60519B7E2DB6E8BF8B48C1F2
28	dfInput	00A13D0A8563DA7EED1BFFA9DE862B4149BF8658EA8DA5034DE52D88E04875EC57F85B55C10DD5B0563BFECE60519B7E2DB6E8BF8B48C1F2
29	dfOutput	73E88D0DD56C78FC0896D5C32ED7CFF0C22ED183F75F9E496EDAEE1939C1CC1A608F7773942440D32E9F9906BD9096FD206616EEAC5E53

30	reseed_counter	1
31	output2	11C97CAD448EF746ACCF1E0FCD526737AF4C85D54F62C216961771 90FF5E377A550159089280404CC6BE780C1CCF443A9A23685C00750A86
32	H	B5059ED4018234C08AF67E20BC0771E05CCEFC7BCDBB97D87B5AFEAC
33	V	152597933946F7E924967FA1B503113A81B52A6E8504A197540877AE87D68C73DB1F8DBF987811E5721047C3DE2890F892E6AEF5501EF2
34	reseed_counter	2

7.2.2 LSH-256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	df0utput	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
6	dfInput	006B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
7	df0utput	9D6B66A8636E1B65248705B2DD0CFDA1A0BB594275022EB49A8B35B57919FCA9CCD43D316D95B30034081 5C46DD47E9DFF600C75631A61
8	V	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
9	C	9D6B66A8636E1B65248705B2DD0CFDA1A0BB594275022EB49A8B35B57919FCA9CCD43D316D95B30034081 5C46DD47E9DFF600C75631A61
10	reseed_counter	1
11	V	6B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	016B1A471B69C4C92AEBDB218411E553F768C312F83965471CCFA99CED27AF39AEEAF61CA15E192033D75D549C18861E03D894B7FB90F7CB92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	df0utput	F79B6384320B0CCF0A8C9AF982C3AAC9E15BFD19FD1641444B3FE09D6D3EA79524A7ABD0217FF6E48B2342223731 58B5F3C2B0C5AF2798

16	dfInput	00F79B6384320B0CCF0A8C9AF982C3AAC9E15BFD19FD1641444B3FE09D6D3EA7 9524A7ABD0217FF6E48B2342223731585F3C2B0C5AF2798
17	df0utput	17339E02AD19E6075A82938F770DB9B173622677ACDFC1F8459863AE0BB4E7A6 A3E826106A91692608F061E32F3634357E3E19783FF16E
18	reseed_counter	1
19	output1	024F79C65FCA980DB882DAB66B3C221EE8420B7B7D4E017B9F39B30111076E70 75963A4D432354BCABF647965B38DED6F522574F5754C355D03C2D0C1470028D
20	H	FD615A87919ADCE1984223FB2897F858A6E478B8369027CDFEEC53D63150CE1E
21	V	0ECF0186DF24F2D6650F2E88F9D1647B54BE2391A9F60439F232CBDD13D070D4 0AB3CD092409B8B1788C5C3BF68F5AEA5E54A06F3FE725
22	reseed_counter	2
23	V	0ECF0186DF24F2D6650F2E88F9D1647B54BE2391A9F60439F232CBDD13D070D4 0AB3CD092409B8B1788C5C3BF68F5AEA5E54A06F3FE725
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	010ECF0186DF24F2D6650F2E88F9D1647B54BE2391A9F60439F232CBDD13D070 D40AB3CD092409B8B1788C5C3BF68F5AEA5E54A06F3FE725F148FD648C2B7BB0 9395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F 27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	df0utput	6C864B72C106958CC9B1EF5B7C89D8CBB3DC4D54F63472D63D04753440222494 A179702F10E9825494A10521CB270410D4B0B46876F37A
28	dfInput	006C864B72C106958CC9B1EF5B7C89D8CBB3DC4D54F63472D63D047534402224 94A179702F10E9825494A10521CB270410D4B0B46876F37A
29	df0utput	EE60AC0EA9C00AA83EBF7841CF231D4E04B60978EE566A27DC468881CCE12CF4 6FE7C95BD63DC3664D000FF2809FF9D79FCA75169E5DD0
30	reseed_counter	1
31	output2	0FF1E27B3B5B2492FB79A397F7370E789331CB0E255A088F914775AA29B0AC16 50808EA529625E2BD3BC45B823A767E55E49ED7CB9ACC01FF02F1342FDDAF551
32	H	8FE42156835F5DEE2C26036F5C7D124D79D48EB9A52874AC8CC859F2F49205B1
33	V	5AE6F7816AC6A035087167 9D4BACF619B89256CDE48ADD8DFD6C54396C613FB5 3764A8E764399334B62FCEB9743BAA753CD51C73A756FC
34	reseed_counter	2

7.2.3 LSH-384 기반 Hash_DRBG의 참조 구현값

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

4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF1
6	dfInput	00E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF1
7	dfOutput	B5E5365A977CA11A5AE9D0EE37A325A920316E2C37726E6EE98A4ACA53ED64B919A69356D639A679D0877E2467939B429676EC676A303F1018A965B21C38672AE85099122EE5826454764D629E1318948BA67ADE9DB7E85D36D4331CDAF990A7E3FADA75E59F144F9D643265ADF07D
8	V	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF1
9	C	B5E5365A977CA11A5AE9D0EE37A325A920316E2C37726E6EE98A4ACA53ED64B919A69356D639A679D0877E2467939B429676EC676A303F1018A965B21C38672AE85099122EE5826454764D629E1318948BA67ADE9DB7E85D36D4331CDAF990A7E3FADA75E59F144F9D643265ADF07D
10	reseed_counter	1
11	V	E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF1
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01E47E11ABB6BAEA6E70A585ED1308F10F9FD6230543F7C77FBF3A746806DC29C29264C9C0FD8FB1E9E32B830792FAD1B2FE885E046903C7763C3AEC1EDF575F0AEC1A7AE948B6EDFF1DE94163CD8E42979B05CBC48C664255E3289ADD0656C8ACBA62997B7BEA6A975D6D256DDCCFF192BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	dfOutput	C6CCD529017F64B079D340908448F0B9B836B47BA7EFFA0A5BF4CE88C47F7743894859364F391D2A1B0C92FF6090D85BD6CF3031354C50600C4643CA7AC27441FA91F532CA18918B3E74C94E8485E0F31D9563A1CE7B8F005897390F649AC6C624FC407598D68046747065897FD58C

16	dfInput	00C6CCD529017F64B079D340908448F0B9B836B47BA7EFFA0A5BF4CE88C47F7743894859364F391D2A1B0C92FF6090D85BD6CF3031354C50600C4643CA7AC27441FA91F532CA18918B3E74C94E8485E0F31D9563A1CE7B8F005897390F649AC6C624FC407598D68046747065897FD58C
17	dfOutput	E2E3F534FA2EB7A4009A1FD75FA01912E946280BDF63446E7271B5EB99A931D329197347 1D0BBC5EAAE3C6E30CE8FF87DBF9F4F001698E1662D33DCEB68D9851D25ADBD6CD57D48A58219B9589BC61DFF8594F98560DD026E3F47546800A2F39AB2294685EBAB32156C0A4EEB84A5A
18	reseed_counter	1
19	output1	AFD7FC874C300A4E2458319ABFED94A4CB15A84A7EB13E2C62C512C32F240CEF87DC0248BF633C51E92B4D9C59E47B816F097D3429D5B958DF3EE8C4C2C590EAD600419F982CB86468892798ED93E73D9BE9196C850F54AD45C547253CE1B442
20	H	FDC39BC0150E74FF421CD105E9116A504B22044D5B5A10444F25AE41F59E2C493778B0AED7EA728EF72E658EB4CF9398
21	V	A9B0CA5DFBAE1C547A6D6067E3E909CCA17CDC8787533E78CE6684745E28A916B261CC7D6C44D988C5F059E26D79D7E3B2C9252136B5DE766F19819931500D919088911EA5E56557B3676ACD1FAC931E37F300957E99A3766239F04B82D13F3748CF83B5E203C25EF996992D07B37F
22	reseed_counter	2
23	V	A9B0CA5DFBAE1C547A6D6067E3E909CCA17CDC8787533E78CE6684745E28A916B261CC7D6C44D988C5F059E26D79D7E3B2C9252136B5DE766F19819931500D919088911EA5E56557B3676ACD1FAC931E37F300957E99A3766239F04B82D13F3748CF83B5E203C25EF996992D07B37F
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01A9B0CA5DFBAE1C547A6D6067E3E909CCA17CDC8787533E78CE6684745E28A916B261CC7D6C44D988C5F059E26D79D7E3B2C9252136B5DE766F198199315 00D91908891 1EA5E56557B3676ACD1FAC931E37F300957E99A3766239F04B82D13F3748CF83B5E203C25EF996992D07B37FF148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	dfOutput	2E672C277DFC4EB66D2A6BD5BAD1D0EF7200D4B25516E474690426D2FC8661E44CDB73F03D1AD9E54B27BA1A92636B701CAE66621D622C72366DB9DE8D8059BBC422F5E16FA95C258A91387FC4469F9C9C71E90314274C627B1A32FC22C3C5175DC063FAAFDD73E82CB4A9A293CB0B
28	dfInput	002E672C277DFC4EB66D2A6BD5BAD1D0EF7200D4B25516E474690426D2FC8661E44CDB73F03D1AD9E54B27BA1A92636B701CAE66621D622C72366DB9DE8D8059BBC422F5E16FA95C258A91387FC4469F9C9C71E90314274C627B1A32FC22C3C5175DC063FAAFDD73E82CB4A9A293CB0B
29	dfOutput	270C739115EF0C726A6E4DED9B63593D253F1D409A14CE78E21DEF5A2491B8D9

		3B1ADAA5EACBA1DF2AFB4E29EC0057D1F7235D187FE640AE192F42A202F19E84F422EB155FB34EE31992EC517F9823347CBC54953566395E72DA8257A1C4008F666CAFDEE46CDACFDE979C3F55E51D
30	reseed_counter	1
31	output2	4BEE112E4EA52C3624DE0038226EF11D5C2D3C0AD32CB7F0B68863F6BB406FAAEFEEC1BC1F06CDF18729A7A05C0CF8A8E8027613C2E97A886B4CF7EC89A416B3A8920A26A8E879E0D2ED8F079142315 39B12466A968B38DE54A285ED911C63BF
32	H	34FD083C9406D8EC287D58A0EEA826080EA736A88FB7E1CF4F3F91D9E74A57D2B4899DE39F771C432EF2F1765BAD1E05
33	V	55739FB893EB5B28D798B9C356352A2C973FF1F2EF2BB2ED4B22162D21181ABD87F64E9627E67BC4762308447E63C34213D1C37A9D486D204F9CFC809071F875B54E1D8AD6359731217CC5BFEC04CADFC064E628016F55102D868F3B0EDF985B4DCAF7790B6691E6FE3DBC3D96CE2E
34	reseed_counter	2

7.2.4 LSH-512 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B
6	dfInput	00ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B
7	dfOutput	BC1648BB27119BABE1D09A426BBC66DA6FA54C1C432AAB80F46C0645492777138570503 6AD4986F0FB0FC73FB1C2F7696256EE93B213D25DDD556D0DEE90E0C5EB74B3DFA65C99FDB60A367577CC06FFA7AAFB496818FF2462F12028B691AEFE8DAB3BA702FA2ABE9C7D5FDE6A1F2E
8	V	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B

9	C	BC1648BB27119BABE1D09A426BBC66DA6FA54C1C432AAB80F46C0645492777138570503 6AD4986F0FB0FC73FB1C2F7696256EE93B213D25DDD556D0DEE90E0C5EB74B3DFA65C99FDB60A367577CC06FFA7AAFB496818FF2462F12028B691AEFE8DAB3BA702FA2ABE9C7D5FDE6A1F2E
10	reseed_counter	1
11	V	ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01ED64FFE8C0EB192F1637CB59D2AD447188952F1EBE5A6F38F475B95A1B916EAD72D32ACDDF2F26F3A454F0006389300E7BB8051F41BE571A87A73FEBB4698A5C92F4FC532222AC1F488A000FCF114E7E2F08585CD687B8C3F61510512A58AF619DCE974E8B63E92DCAF22631399B5B92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	dfOutput	48BC9E171199FC249E3FC88C3814CA702213F996B12E4E2BE1833B7E003593F1D9F6BAC7875694B9AB7EC78096F5F11D548070C5DA085BB86E4202EE1BB433A75B784CF90F8F04ABEE51DE86E1D1B262A060B6E8F39432B9A4F6872A32EC55AEB72ABFE6B420C82E501ACBBF4052E0
16	dfInput	0048BC9E171199FC249E3FC88C3814CA702213F996B12E4E2BE1833B7E003593F1D9F6BAC7875694B9AB7EC78096F5F11D548070C5DA085BB86E4202EE1BB433A75B784CF90F8F04ABEE51DE86E1D1B262A060B6E8F39432B9A4F6872A32EC55AEB72ABFE6B420C82E501ACBBF4052E0
17	dfOutput	9ACFCCDEB0E9B022A4324FF2A371377BC15DD5D59D35874859F4F6DFFE36549CBFD6807CB7D81A1BC7D7E54ADC3F21511E2AEE8075E5E14BEDB700B685211FC83F53753853C4226AADDF459FD8C7C64DD214C806B458264 1B6359526A4AD4369D285F46FE166D788B700916BB7AB2F
18	reseed_counter	1
19	output1	718918699B69DA7EA591835674F4FA557BBA51471747883E7F12419E4C06A5AA1CD3994D229CBEAC31AE861D445DE2A2547D6C34BA9E5C6ADEF61C25C9B53B9FF9DE6B645D99435DECF4C1E33506072AB98D4A64DC245821EB763DED27B73F687B1435F10E5B1258ED80B3E8796193C1461E4309138B0D462E4D412DDD216F56
20	H	ABBB9269334F01A572CF6CD05867D02C9EAA149FEA6D7466A96BB10A833DE76D632238D66A92835D115A97E5B8FF23CA127658BB79D91E8F7E88FE63FF9BDCA1
21	V	E38C6AF5C283AC474272187EDB8601EBE371CF6C4E63D5743B78325DFE6BE88E99CD3B443F2EAED57356ACCB7335131A2E3DC8799EEFE2772B65D3FD08A5800E44E0621BD0C78DC007E22EA9F880E61394AE555A3A6FB60CB5C40209D6BD632B00096FD06EA62F359019C12A93DAB1

22	reseed_counter	2
23	V	E38C6AF5C283AC474272187EDB8601EBE371CF6C4E63D5743B78325DFE6BE88E99CD3B443F2EAED57356ACCB7335131A2E3DC8799EEFE2772B65D3FD08A5800E44E0621BD0C78DC007E22EA9F880E61394AE555A3A6FB60CB5C40209D6BD632B00096FD06EA62F359019C12A93DAB1
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01E38C6AF5C283AC474272187EDB8601EBE371CF6C4E63D5743B78325DFE6BE88E99CD3B443F2EAED57356ACCB7335131A2E3DC8799EEFE2772B65D3FD08A5800E44E0621BD0C78DC007E22EA9F880E61394AE555A3A6FB60CB5C40209D6BD632B00096FD06EA62F359019C12A93DAB1F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	df0utput	040A46B569BC566BFB837960C8055319D77E5CB59E8151F5D554D3C133FCE3161EB6AF1C89626C4AA158FF6AA54C43C3B6497EE3A340EB59F0455416ACD1C6D861BD4B985C52FEC952B50E452A3FD34A19E0CBC74A7384AD41AE1CC9A9E04EA665411E82F8DD1DE018BD41535AD295
28	dfInput	00040A46B569BC566BFB837960C8055319D77E5CB59E8151F5D554D3C133FCE3161EB6AF1C89626C4AA158FF6AA54C43C3B6497EE3A340EB59F0455416ACD1C6D861BD4B985C52FEC952B50E452A3FD34A19E0CBC74A7384AD41AE1CC9A9E04EA665411E82F8DD1DE018BD41535AD295
29	df0utput	94B46A437E4CFA9C5F09C12803E52B4CEED8E7D0369C3DFB83E0D0DACCF99BCC13BCF2C66C6D67C3818CCBBC05052A4E66F4306230219B7F524614D6E88F643D1051A14FC159331B461E40F85515A62A371BF4FE30D3F4312B00C10B6C679902322A1880C5DD71EE322D9BAB4997C9
30	reseed_counter	1
31	output2	D69C62E2D4761861CB8CA3C2808BBB0E70B03C1E29456528A021DE683D85A5AE42F833757B289476F8DF74C57C934EB74E95330820DD8701F5682A4ABAF2A60281AC9CBBCA8F3369308234F68707BE4DEB2CBE5107910ABE46FF8F57D71AD8F08FB1A60D0D6D2BC0A9F2EFCD353DCB9D962014FAB7189E23DCE3A89A70E2AFAD
32	H	4956574DB2A92F908A88D1225CD01AE8131B53A3E7BDF8844BBA1FFBEED289ACB1F6EAAEA584C5543C7FCE12DF6FCD1EB8647581D8A41C79F98960F446851340
33	V	98BEB0F8E80951085A8D3A88CBEA7E66C6574485D51D8FF15935A49C00F67EE23273A1E2F5CFD40E22E5CB26AA516E5B7394FCF87C921763CB5C8B4A657C13288D6290CFDBA4B63052F34B2C51DF262647E76F6B000CCD1AEC7CF0B486150660FBE0B8DC62D709C7D44BD145297D9F
34	reseed_counter	2

7.2.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	df0utput	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2 CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
6	dfInput	00088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112 D2CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
7	df0utput	6F8809E884E7142C7FB27A734CA23410157FD2188676A42B44D5D4150C6079E0 09B6CAC568B51312064C5F696EA61085D63D85A10A569B
8	V	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2 CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
9	C	6F8809E884E7142C7FB27A734CA23410157FD2188676A42B44D5D4150C6079E0 09B6CAC568B51312064C5F696EA61085D63D85A10A569B
10	reseed_counter	1
11	V	088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112D2 CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD1
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01088DFD426F56F7554D2E2357C5D9A301D99410B626E8757CC89BBC7A97B112 D2CEB4B9F6B4E4D030CD303E29754C03DD72EBFF0583BCD192BAA7658C23A7EE 8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C6625B06B16AF81E7 13A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	df0utput	A2EF3E14C2F0364046E13918BCD6B2CF6397EA596BAA27BD9FE2674A74C3C59F F31C8C7FE579FBDF7D5A555472482F71714026B4FD9A79
16	dfInput	00A2EF3E14C2F0364046E13918BCD6B2CF6397EA596BAA27BD9FE2674A74C3C5 9FF31C8C7FE579FBDF7D5A555472482F71714026B4FD9A79
17	df0utput	FF2455507F5CDD1967DF5871803DD38DA1DED174B4E9DC7FF7860A5AF7826CFD 4FAF6DB1EF33D79514D7FA29B9A9EF55EB420486F9BAE7
18	reseed_counter	1
19	output1	110DC1B66AB64ABC5A753B87504FFA2A122DEA80F88126670ACB0B6110C03806 70A2A40DA48FD4DBED60AD694960D90C8EBEF63D3F4FCA78
20	H	9A8CF12BED80B8DBB123E929345533E9FF2F4608017C6B61DA489863
21	V	A2139365424D1359AEC0918A3D14865D0576BBCE2094043D9768723FF9375E8A

		C384D5E2F896FCA8E766397D5B3826C8D8ED8D163FEDC4
22	reseed_counter	2
23	V	A2139365424D1359AEC0918A3D14865D0576BBCE2094043D9768723FF9375E8A C384D5E2F896FCA8E766397D5B3826C8D8ED8D163FEDC4
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01A2139365424D1359AEC0918A3D14865D0576BBCE2094043D9768723FF9375E 8AC384D5E2F896FCA8E766397D5B3826C8D8ED8D163FEDC4F148FD648C2B7BB0 9395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F 27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	dfOutput	723DB4C670E511F0B32E2624D081E519BA04FA38EB0C0C3897589B5EFCE3D7AD BDCB794E372C55FC63DFDDF18F25C36FE805C53D0D56CD
28	dfInput	00723DB4C670E511F0B32E2624D081E519BA04FA38EB0C0C3897589B5EFCE3D7 ADBDCB794E372C55FC63DFDDF18F25C36FE805C53D0D56CD
29	dfOutput	A4FF5B0CC8400FEA634F7220BC59E5A73F6DFA78976470EF8F4719BB155BD89A BF82DC39D7ACB495E5BB8955F57E177CD36232DA9E5673
30	reseed_counter	1
31	output2	AA2DDE4CB37675B8CDF012073A7EEA34A0584FBD96959AF0E61AD595A8BF5CEF 466E119FED2608755FE985D49DFBE9C899020BCBF86B7276
32	H	B9736B7103D01ED5BDD22442FEB521F5BAD73C3078942A0DF689FC52
33	V	173D0FD3392521DB167D98458CDBCAC0F972F4B182707D28269FB5D385AB214C 4D6D2B45E0FD4D90FEBD5D025BE00B654F92060E35A993
34	reseed_counter	2

7.2.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21 BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147D E010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE 025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
6	dfInput	00709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78 FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
7	dfOutput	A7BEFCAA9C5CE75BE8DE729DFB1955DBA0001D0E2E1F155E879560897CAEA42F 7DF963C35DDFB560C76988C1016FC09500E7ECC87038E6

8	V	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
9	C	A7BEFCAA9C5CE75BE8DE729DFB1955DBA0001D0E2E1F155E879560897CAEA42F7DF963C35DDFB560C76988C1016FC09500E7ECC87038E6
10	reseed_counter	1
11	V	709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F0
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01709B4FC7757F739BFD33872E36EF10823597958E0A9AC036BD0DB5E3CE6E78FE025D62F1A33D2378A9C5676B2C6F01ACB66863F971B4F092BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	dfOutput	0D50A0DBDE8A5ED04BB6849AACAEB2C7C4E964B3BA8349959BD00E0999113152681B117681ECDE587B6530B142AE80DC05C152A65A9F70
16	dfInput	000D50A0DBDE8A5ED04BB6849AACAEB2C7C4E964B3BA8349959BD00E0999113152681B117681ECDE587B6530B142AE80DC05C152A65A9F70
17	dfOutput	ACCD177F496ACBC34A290400B280F46ADC846D4CC737AC670A6259FF769A29DB2F0BD7798EF43FE04D802D490A64CB2F9A1E7CF53E05DB
18	reseed_counter	1
19	output1	A2C93A67B042B03CBF79CE9A25FD1D7C5A87DB87C03ECDA9CCA4739357EC2E62D617E7BD168A66870756CF098DEF85F5FB1B30EA13A147FF7CF794E73FCDE10A
20	H	BD5D62802CE78199580420D68943F3E91E17CCC5250C6F17C641C1746A335E62
21	V	BA1DB85B27F52A9395DF889B5F2FA732A16DD20081BAF6BA0394E835F72CF4859B47BF7954D50756E0B2231F598263D1E1A14405CC03AE
22	reseed_counter	2
23	V	BA1DB85B27F52A9395DF889B5F2FA732A16DD20081BAF6BA0394E835F72CF4859B47BF7954D50756E0B2231F598263D1E1A14405CC03AE
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01BA1DB85B27F52A9395DF889B5F2FA732A16DD20081BAF6BA0394E835F72CF4859B47BF7954D50756E0B2231F598263D1E1A14405CC03AEF148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	dfOutput	5184EC5B8EE079D7A6C6DB8674A217EC9030O1B16F27FCF6FDE6A40872A2A1C0F7EB62C5DD42711B7DB96EDB18B80992F8EC4A4BE04A90
28	dfInput	005184EC5B8EE079D7A6C6DB8674A217EC9030O1B16F27FCF6FDE6A40872A2A1C0F7EB62C5DD42711B7DB96EDB18B80992F8EC4A4BE04A90

29	dfOutput	867DC0311D3F2E7BA03C6C9C9B5D71BA175B0D2F2367230145950EB46067A9E4 0467565E692BE088813ECE0FADD8688FCA41A3CC102162
30	reseed_counter	1
31	output2	6B07CA5C0308B7758E5AFF53946D53BA427FD322F4E0646628DF191B900276EF C70567161C48163BFD1B9DDCC4BF1AD9F23732103A6681C3FE1FBF94FD1F719A
32	H	2541C9A6F7E5E7EAAB7FA4A413334E6807F2CF5447491F7403893E7916B8127B
33	V	D802AC8CAC1FA853470348230FFF89A6A78B0EE0928F201D854559B4B8F23650 7BF75D3779BCB9ABF1C791320FAFE6264C6C672EA87E6E
34	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 LSH 기반 Hash_DRBG 참조 구현값을 제시한다.

7.3.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	4E9D8020AC087CA0A32E134F0A88BD878A976F9B1E000C04DEAB8BE413471A69F1A2560C06E03648EC8E004076D7CF23216ADE670E4C8E84
	output2	F435A55A55674D749B82B9010B27CE34780A4C8AF4E6A4C07AE6628227AAA9FA74741F7156ED230786417D7E0732FD5B3655F6D4F810DA6E

7.3.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	6A61AE300967547E8F2175C02E1346C68F2065BFE8B5EA9FB3AA3A15BC5FAD22B1AEDEA4C8C4FE04765036133486 57C3460962ABC629651CE07C9BE83A4C9292
	output2	56ADCE01948B6D96418255ED80BE5B7E22566002249837E52927FB4EF7DB43B0DE68F997208F4235D740FADF1B6738C9AF90D593D1A1A1E7E2A13EE54A5795ED

7.3.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	32684FA767CAEF3390A6A7CB7DB1BCEF7A71EF669144AFF84084E141413808486BF334FAFC852101A48067C0FB41109BD5B4E9C314FFD2D7EAC044B0F7D20EFC0F2740C4E1A3819DB4F31CFE56D10D597A2AB9A9C4C55AAE3C9663D7A04EFD7F
	output2	BFD30A96D1EB506B5AEFEF53572F015E19BA094818F4B3A4283911E8E1FB428F693433776C6DE9C79DF26972414C78E038C8E962824C2851D14F26D79B83C8CA70D01DA6E895971F583AA267925342A4113BF3C5A61408EF2A245D5CDA114E9D

7.3.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	915AEC0995C6FD5495B7E5BC65D80DE7A6913E354A8265BEBB8B031F571A88FCFABC5175DAAEB4CB94E17AE846BFB81B447E58C0DE13A0E6E889C42E0A8971EFC64D30DAA1B86AC980578DF61CC040E44C24D0AEB82FF4ACB5B0137098B150BE0FC6EDC67FA06CC29BCADFD9FB5C27D48A2840DAFD71BDF67AAED3D78950521E
	output2	AAA8900099D1889D9BF8CA9A7A5DC83D6DAB350687606F780B8CB15D231F5A5E3637AF484A59381724772EB84898992BB9C4DF0466A8BCAB8655B8DFA04279F1C741A3502E08A3A510212A14122FDF45AB6A9DE0EFF6E0F1E72A7E3303889F635A02E5CCFDE039C6A7AC1142572BFFCA309CC2B03B1D974335D140796AE2AEF6

7.3.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	16E7B48E6C112CE24960C8DF615CDA1C09BB8766F28FB8F3C95C44E4EA7D9FC0 20F7D6BFA51B8CA4FBA731FC44C14AF3D6AE34A206BE13B5
	output2	BFD3EA6D643132038637FE0ED04D17BF84CA2D93071E53F334046DF2039AB4A5 02AF1EA83182DB550E790D67603C95C7F9354181BFE52D00

7.3.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	B47B9D5FB12926C5ADD90E1A8DE505E987A6E248CBC427D0B3335A74EB8B8E64 7665DE5457B8B8E227E05D52BD1AAABA91F458454DB4D28D6A6D6B12C63BAB9F
	output2	B2F07D9F4044E1B0979AE285FA7F6924E447ED576A132B6166240A05BC35B7AB A5FA7ADDAFFFB7430095068BD1949D34123D8F2B886490BBA8E8D99CA5241BC9

7.4 시나리오 3-3 (개별화 문자열 사용, 추가 입력 미사용)

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

7.4.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	3E51C202AE82E4C1B2CF16739074AB282DA82D0F5350A8985AA1B65F6D4F1D583518F327C3B8CD2C732F3CF7CC3F1718B3EB529A3DA2C4D7
	output2	305F79DA6E33E98C79B198B7874B0419803EA1506CCFB16CDF5A19E4FFBFB783A2C7DCDE3BC19AD66AC3269B0868B80EC8E84F237B216DA1

7.4.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	9E9918ACC65CC0F0111755DD8B3EC9937BF2268370928EF13C755CA021D2CC782E84CFF748D0E72C55154A922FA5533596F709B5D42D8D91E93975F46077D549
	output2	30ECF39A0A1EC68740C3A605150D184086020FBFEB91982D0B600849EB2845F006B37854F5EA849D830BC8A48CD1576E0764436580BFCABD33842D6C2216F4EE

7.4.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	DC453C491DDCE2E619D7205E6D56A89445B01D37F4826EFCE2548745889C47E59E5070DC2A0B90FA1EBA6F1900FB170569554401E47316456076E0C5A550B67AF95E9219068C2B8E8FE243F680ECEF94978896E2987928C0C616D5947B881E7B
	output2	E5E539F495246A065761ACBCABC6C85228CE0B665C1361352FE559520937DA8E6C7E02AC15B51CEDC8AAD68CDA13648967629F3903420424BEF1E3A0A2AD4479ACAC28236F4D5A42F16EE34AFB0317EFD9E6B01BEB776A1C6EE5980C08FEC02B

7.4.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	20BE4C0589E15F832DC6C0436F4F104FFBA8AA33D53C168EF52328795BBEE2B51B70EAE7F522943323A6A2E6E5F3F955E39ED16826F9A5F7288155721576DABBFE55958B96EF7AAD0824408A7CBCDCAC6D99BC13AE65C5AE30547398933AE3C4E62A3FD55947376A5D9E0A67C1A66193323EE2BE6A12D60DE299D363BE3091AC
	output2	5B3178128AC88E351EA82705BDB674740F89EBE823662B6AE491A9C044A451D6456E884D01D0C61C6FF86CF91D0744285958720BB050F766C153C7E29C0CF434EDCB19ECAA7778206B5A2438147EA915313145B93099ABEFBD3B17055F7F98120A658D3CC6FD6E3C3EC63E731E1172443E8935DCE2FACAEA80A4585DF0737E53

7.4.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	56134344A9A36D99830BBEC703E05EE347223D14F5EE6B465FAF2308BA53E15F A5F9D5C657D4A300BD6D3D13BECD0DAB35BD432F568B8486
	output2	B707304180763B43DB561471A3386009688557E88C88DBDB0D1BD19DCE22080B D44EB699369750CF862F070E1C744F34FA6C67E1C931C1C7

7.4.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	063FDFCDBC0FE53799BA147CA9C9FACA7F8292C49E879F4F9902F923D99298F9 7A82B8265C5A395B9090CF868399AD527830A2F0C0483BC71479EB350BC59C17
	output2	CD23809CDE04315560D6244364C57DF68BA396CB74AFCB5871EFD011AD60BF7F D78A80C3E904790703C3918E6957000209DB2CAE00775AA4F219D2BD7E57059E

7.5 시나리오 3-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

7.5.1 LSH-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	5B3EEB8427A1F282B860AE708DB7E43CAD3F54F8D35E3540CF89EF90677E2726BE5265D562BC8AFCA2970EA5D84D1DB577EC192A104BE047
	output2	1FF25A59A107E1656C3E707C0B8BA862A66F2943287037A151614FCA2F52F5CCF9420C9C8F1C3EA2084157357FBD7B885F704BE285854397

7.5.2 LSH-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	E2C554B44C1368B87CF536F56CA7F376A1642FF9335039252ABD54E6AC91BF67E5D455D210E025E72A4C1CD6D8146A03AB25BE76E0E92D0CE139A5D254358C1B
	output2	FBBFC96EC03E045B01270125C16F9F93DA546CAE0383140BFB71DD11A130F898EFE538AC768B3197010F40C62999677B1FF9CBBBF85530C2263D53F0B5923567

7.5.3 LSH-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	C283F7037F2A525ECF958EE08D36748D9F3AED3F4A8E55DB11F46584573C35369F929CF9B3B1CEF4162228817DFF3F8A57608889FB8F4E13D5D218900C6BD9285DCE51BC2EE7F59AC82291B3A7C4BCE6252248A39F6A346FC7E1E01CF7369835
	output2	041D851166794047A15E29E75184AA7ADCBC58F2F100F61CD28FC0AB43033BE1497018AC50448147FDB4A04A789C436D79B4417E8465FE88330C99BFD556ADD96EA9386746B13A93CD0A5841DB5251CC308B315546A2E0D2E65AF4F84010C871

7.5.4 LSH-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	154EB64AAD4D77AEBD26999BDCD72A60456BC02309674784626F60411AAFEA7B5A6B44DE2DF8641A32BA1518341109 93F1D07210640AA1322AC7FF12107345D6DB98DFF76A51E9C3C6885DA0E8EFD215DA01887228C3B26C805CDAE7459CAF53A7DCCD786A3670450692DFF3364C0076E31FCC53828CBD38D7C9DA0F27B6AC1C
	output2	2CB4005FF0B3E3153F00DE052B36185A063A2F8ED0FEC9E1FA0C4A2AA0E8E1916DAA739C14ADC3A0479C00DBBFF8A99DF4F09D35F6757CEC21F5AB63FE3E39F6BE1A97A03E19C8B34577C6243033D16A385FE63F7349149DBB5326F0DF76B8F8A3948BC5EA90FDD18EB411A6E78AF51160DEA2A7CE7BF407A34A581F0A855FA2

7.5.5 LSH-512/224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	EB402C46A5BCDAE92E4C15CBC0F4A2D85FF8009B9B7984B284EBB534AD217B0A BAA413C587071CE86033A53373F7DAAB156430B0CE1346D4
	output2	D89008CD2715AE86E3132EB41F151528876E7B3009B0401D088111301C3CD10B E4C9599203B93BD5CB3B1D98077B525E0167A9C8426F4442

7.5.6 LSH-512/256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	05F35CB432EB50E36018B2797EDE0156A7D33A938BCC5A71178D20A662B3367E 89E3E1164C3C78151AE568EB6383C334EF013E40D1B5B1293965022FF1D076AF
	output2	CE273529C1DF21CB809FA1FF68C49A51A5B5B38C94A661A275060F3EEBD94EE7 D7DA64CF74217CE019649F6C42FC3600142221F62BF7A610F8E2655E919A64DB

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.

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

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.xx	제정 TTAK.KO-12.0xxx-Part3	-	정보보호기반 (PG501)