TTA Standard

정보통신단체표준(국문표준)

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

해시 함수 기반 결정론적 난수발생기 - 제2부: 해시 함수 SHA-2

Deterministic Random Bit Generator based on Hash Function - Part2: Hash Function SHA-2

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 정보보호기반 프로젝트그룹(PG501)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part2
표준 초안 작성자	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part2
	김동민	NSR	연구원	-	TTAK.KO-12.xxxx-Part2
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

서 문

1 표준의 목적

이 표준은 SHA-2를 기반 해시 함수로 사용하는 DRBG 메커니즘 Hash_DRBG의 참조 구현값을 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, SHA-2를 기반 해시 함수로 사용하는 Hash_DRBG의 참조 구현값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 제1부 일반에 규정된 DRBG 메커니즘인 Hash_DRBG의 기반 해시 함수로 ISO/IEC 10118-3에 규정된 해시 함수 SHA-2를 적용한 결과로, Hash_DRBG와 SHA-2는 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 SHA-2 about implementation conformance.

2 Summary

The standard specifies the test vectors of Hash_DRBG used as hash function SHA-2 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 SHA-2 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 SHA-2 conform to the specifications of each standard.

목 차

해시 함수 기반 결정론적 난수 발생기
- 제2부: 해시 함수 SHA-2
(Deterministic Random Bit Generator based on Hash Function - Part2: Hash Function SHA-2)

1 적용 범위

이 표준은 해시 함수 SHA-2를 기반으로 동작하는 DRBG 메커니즘 Hash_DRBG의 참조 구현값을 제시한다. 참조 구현값 생성에 사용된 해시 함수 알고리즘과 주요 Hash_DRBG 파라미터는 <표 1-1>과 같다.

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

해시 함수	SHA-224	SHA-256	SHA-384	SHA-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 1-1>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 SHA-2를 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)	1011121314151617 18191A1B1C1D1E1F 2021222324252627 28292A2B2C2D2E2F
	entropy_input 2 (entropy2)	3031323334353637 38393A3B3C3D3E3F 4041424344454647 48494A4B4C4D4E4F
	entropy_input 3 (entropy3)	5051525354555657 58595A5B5C5D5E5F 6061626364656667 68696A6B6C6D6E6F
논스 (128 비트)	nonce	7071727374757677 78797A7B7C7D7E7F
개별화 문자열 (128 비트)	personalization_string (perString)	8081828384858687 88898A8B8C8D8E8F 9091929394959697 98999A9B9C9D9E9F
추가 입력 (256 비트)	additional_input 1 (addInput1)	A0A1A2A3A4A5A6A7 A8A9AAABACADAEAF B0B1B2B3B4B5B6B7 B8B9BABBBCBDBEBF
	additional_input 2 (addInput2)	C0C1C2C3C4C5C6C7 C8C9CACBCCCDCECF D0D1D2D3D4D5D6D7 D8D9DADBDCDDDEDF

- 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, SHA-256을 DRBG 내부 함수로 사용하는 경우 DRBG 출력값의 길이를 512 비트로 한다.

- DRBG 운용 주체에 의해 난수 생성이 2회 요청되었다고 가정한다. 따라서 SHA-256을 사용하는 경우 512 비트를 2회 출력한다.
- 각 시나리오에서는 씨드 생성 과정과 출력값 생성에 영향을 미치는 선택 입력인 개별화 문자열과 추가 입력의 사용 여부에 따라 참조 구현값을 생성한다.

이 표준에서 다루는 세부 참조 구현값 생성 시나리오를 정리하면 <표 1-3>과 같다.

<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-12.0190-Part1, 해시 함수 기반 결정론적 난수 발생기 - 제1부: 일반, 2018. 12.
  (※ 이 표준의 용어 정의, 약어 및 기호는 해당 표준을 따름)

3 용어 정의

- 해당없음

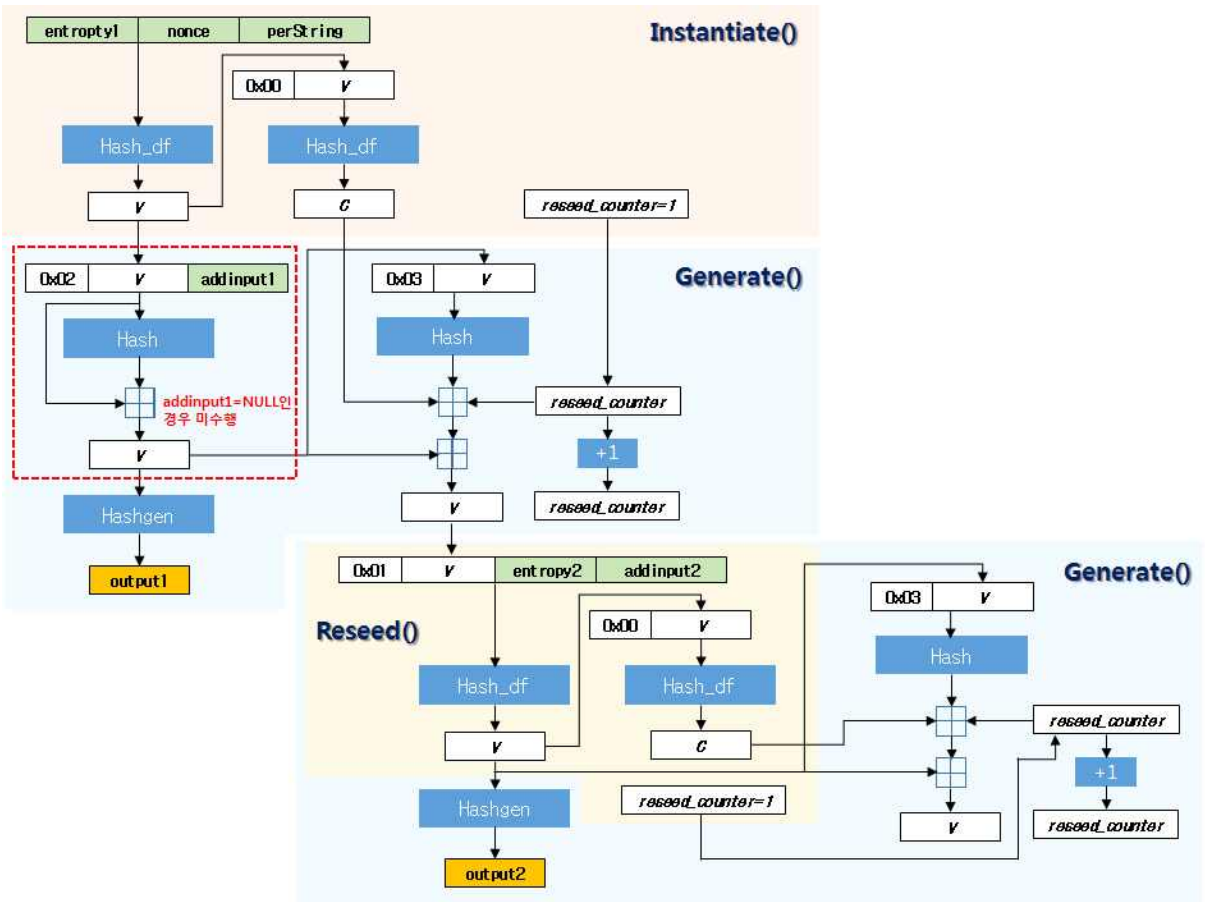
4 약어

- 해당없음

5 시나리오 1 (예측내성을 지원하지 않고 갱신주기를 1로 설정)

5.1 개요

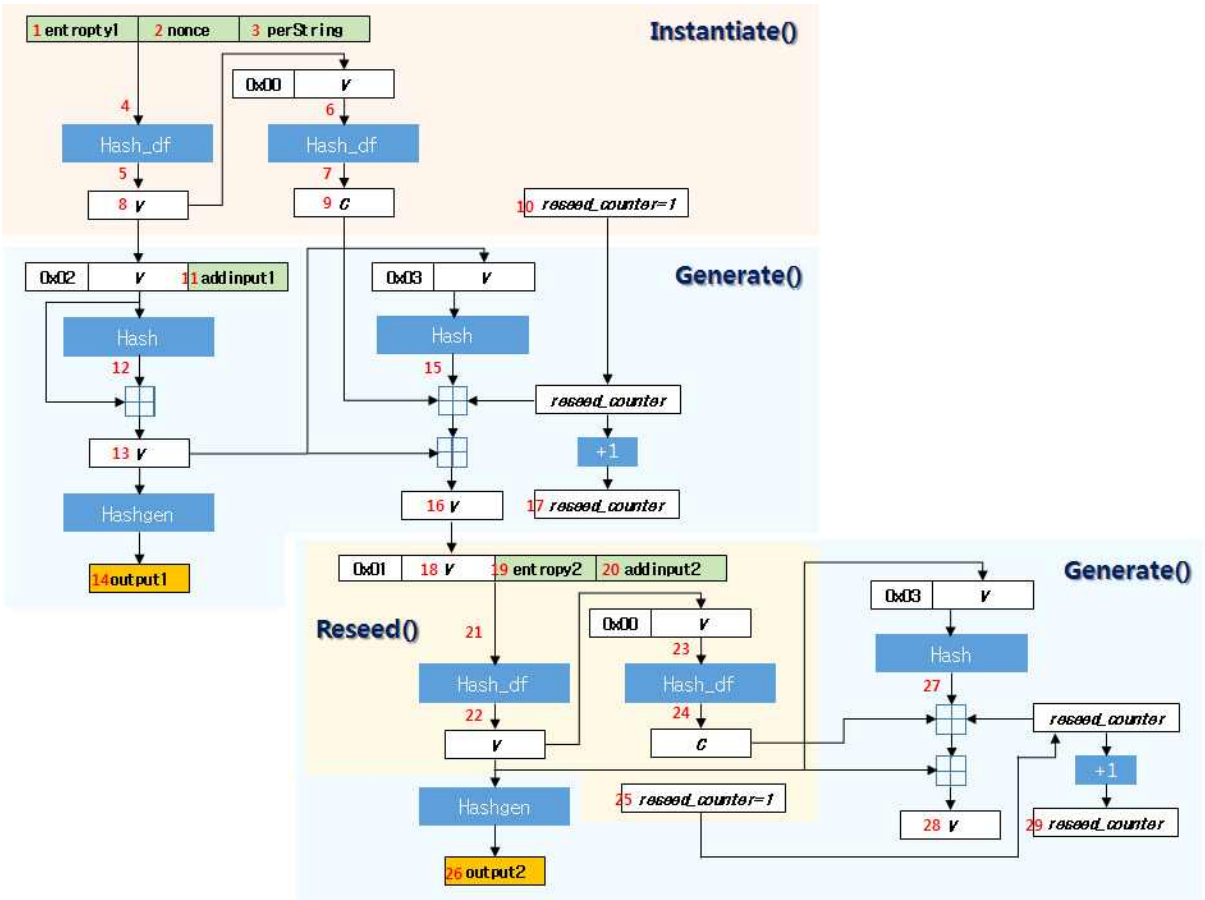
시나리오 1은 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 1로 설정할 경우의 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다. (그림 5-1)은 시나리오 1에 따른 Hash_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(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 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.



(그림 5-2) 단계별 참조 구현값 위치

5.2.1 SHA-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	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A 70D8B661CE5671D8831811F5908C278197BACD0BAED54A

6	dfInput	00E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
7	dfOutput	DB8C7A562E84DD05AC997876D9F525DA924729686861 8E0FE7F04E5408210761707EE2C4B6E3E18D276A434DBA4F961360F72316281DEE
8	V	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
9	C	DB8C7A562E84DD05AC997876D9F525DA924729686861 8E0FE7F04E5408210761707EE2C4B6E3E18D276A434DBA4F961360F72316281DEE
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	FAAB7AFFE93A64020803B5E50172C8740A17422FFF522770CFB9AA77
13	V	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4711D5926D5C43AB3CB869D20C56D9F5E085FFA7CE5780E9E23DDB687FC1
14	output1	FCD78232ED6A1AF0F3292FEAC467AA5DCB34FEE49A6276B0D57AA713F6EB998816F3A78EB8BA38ACB20D2BE1BD272A6347B90B639A80932B
15	H	629825803D7740C8196F8A2E38EFEA8BC9C1D40FBB8880D5E36117C8
16	V	C28F0B5EF2959C812C2622B7685285B0CD5B91BF3D4D1A4DE337608C32B3E3E292FC6347F87A66A00D35551723F1FD4FD35A36D4F1B578
17	reseed_counter	2
18	V	C28F0B5EF2959C812C2622B7685285B0CD5B91BF3D4D1A4DE337608C32B3E3E292FC6347F87A66A00D35551723F1FD4FD35A36D4F1B578
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	01C28F0B5EF2959C812C2622B7685285B0CD5B91BF3D4D1A4DE337608C32B3E3E292FC6347F87A66A00D35551723F1FD4FD35A36D4F1B57892BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	FFD6D33CD6665E60B259AC6314798A8EA1A0DE3C38D814662974F899E2333E6ACE6A90DBB1B105370375EDC14BE23218A2D20CD6CD0BCD
23	dfInput	00FFD6D33CD6665E60B259AC6314798A8EA1A0DE3C38D814662974F899E2333E6ACE6A90DBB1B105370375EDC14BE23218A2D20CD6CD0BCD
24	dfOutput	20D61A3E859093F823542E2CF06186D71060EA3FA48CA3EE840F2FA357569F1EA6771B8DADE75478219D5A78A554252A5734831B7EAC36
25	reseed_counter	1
26	output2	CD35CC38856B8A0067B07A303B47241CA3E44E2BADF275728C582F17021212A5

		94E2A9CC14217883E67565E43BDE2ED1C7A8012E983B1A5D
27	H	A25E3F4A5E5462A17C243B8E56BDFF86AA38721789ABE5BF54D9D6F4
28	V	20ACED7B5BF6F258D5ADDA9004DB1165B201C87BDD64B854AD8428DF97C927E7C9444DE583D3E805E312CEE429A86ECCA5EC4F47258EF8
29	reseed_counter	2

5.2.2 SHA-256 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
6	dfInput	00866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
7	dfOutput	B627EC63298B14586333A30E8FCE253FCA97DF307830DE41F3CC48C41AD1E169E68BAE253140B1A2C8CD4AF8C6B644CDBBD99C6BADF0CD
8	V	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
9	C	B627EC63298B14586333A30E8FCE253FCA97DF307830DE41F3CC48C41AD1E169E68BAE253140B1A2C8CD4AF8C6B644CDBBD99C6BADF0CD
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	1FC204DD477216A2612E03D4BD18A45E7B95AB876CE5C4CCA27233953D7AAC0E
13	V	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E8E4BC9A4348D00B26FB5426723982 45DC66D7C241211699FBC99C76600723222
14	output1	DBEF6ECDEFE741B5EF1F34BA68384F6D5BBD7DA777429D96C74693A8513EB4BCBCC461B0C755B99493623CCDD31E3DE12281F5626BA83AC64594F51326C0068E
15	H	847777A53FC9C793831FFC547215C656799C6E9006B22682932B5175D3D736AD
16	V	3C8B2D67692AAB07B3DD2F4B4687E261011D8305BB050D54B70D9238719A275CBBCA69BADF2B65E2D2B7FF118A46671D80F2783FF7599D

17	reseed_counter	2
18	V	3C8B2D67692AAB07B3DD2F4B4687E261011D8305BB050D54B70D9238719A275C BBCA69BADF2B65E2D2B7FF118A46671D80F2783FF7599D
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	013C8B2D67692AAB07B3DD2F4B4687E261011D8305BB050D54B70D9238719A27 5CBBCA69BADF2B65E2D2B7FF118A46671D80F2783FF7599D92BAA7658C23A7EE 8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F 27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	06F8BAE2E78315EE31D555FFF8095D3EF9E244C7105E36C3BA4BA18F5AF1E652 047E830CBECF55F44417CD02ACB62F8319FDBB4BBB72C3
23	dfInput	0006F8BAE2E78315EE31D555FFF8095D3EF9E244C7105E36C3BA4BA18F5AF1E6 52047E830CBECF55F44417CD02ACB62F8319FDBB4BBB72C3
24	dfOutput	2F699362539ED8B58A39A874A6E101EE5DC7A6045475087833C8C06A730333AC E48F902C7A3F31EF07A2CC66D66DB22FB952569FE42694
25	reseed_counter	1
26	output2	A153B0652E3C8F2E2030B341579F8CCC10D8008DD8F7F8142BE86D374DF38984 EDE45FB7CE32F6832621D9651A72CCA29207CC11CDC2D3C159F4C2C1E778FC7B
27	H	5F42315FA9A523C0E310E91EFCCC8C6F97E40396E776B78B4EF6D0E1657F1178
28	V	36624E453B21EEA3BC0EFE749EEA5F2D57A9EACB64D33F9B3045C1A37318DAE1 F9F73236059AF77B2FBE3050F9DB6D01CA20F3511EAAD0
29	reseed_counter	2

5.2.3 SHA-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	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7 F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74 D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA444 0C59237FB5FEB31B218AB18ECD701F

6	dfInput	00F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30B C7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A 74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4 440C59237FB5FEB31B218AB18ECD701F
7	dfOutput	840906E9246966BFD894747AD536AAB45E0804C785F29D18151EFF128515A80E F0D7ECCF74D44AC6A6AADFD59E5A49CC7936B6A4AA4CADEBE97B8A24E6801EFE A1DB67B49B74F4CE9BC49DFED0CF2C5C9556793B99B0D5D13770F94AFEF17844 08980223B8CCF6E40EE4528BA993D4
8	V	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7 F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74 D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA444 0C59237FB5FEB31B218AB18ECD701F
9	C	840906E9246966BFD894747AD536AAB45E0804C785F29D18151EFF128515A80E F0D7ECCF74D44AC6A6AADFD59E5A49CC7936B6A4AA4CADEBE97B8A24E6801EFE A1DB67B49B74F4CE9BC49DFED0CF2C5C9556793B99B0D5D13770F94AFEF17844 08980223B8CCF6E40EE4528BA993D4
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	765FA8D70A4FC126755AAC11869415A405260D48193F7D5F1530177BAA7105DD 44991BA705F2B296B60A11B44803838B
13	V	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7 F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0AEB 38CD0C5638B388EB379477AE09696C05C039CBA4B9CC6B4452BC8FCE5CA48188 A574CA85A8B149D12B9C65D6D0F3AA
14	output1	1E7809BD9BD6C557FFE5AAF7928B01C265CE644F7A7C79128A2BFCFE622F33FC A15D73EFA595F56537126F3F2B18A74C33E2788745321 16BDA44C563020FBA82 11364878B5261C29BE929334FBA9B399A1322EF295B221FD88D185C1FD0C81EA
15	H	AAAE54C2D6C8E25B080212E26BB71AC4BE0359E433CE9194E7AF0101CF0D46AB 8B43BAF87A9FB8F33B0F573F559CB46C
16	V	764D6C70332A4CBBFF329CA405E08AFBFE8DBC1A7DE622E5BE1CA16835C8B3D6 E0E6485B2FD8CCFF6BBEB6A6B99238B1345EEF84AB9946D79CDCF4F55B7A2A94 88FD36E19D0AD8C1D56BF81891535D2058EA2914220ED5FD392E8AE868DCA557 F1C7C524013733F049D7F7B8173BEB
17	reseed_counter	2
18	V	764D6C70332A4CBBFF329CA405E08AFBFE8DBC1A7DE622E5BE1CA16835C8B3D6 E0E6485B2FD8CCFF6BBEB6A6B99238B1345EEF84AB9946D79CDCF4F55B7A2A94 88FD36E19D0AD8C1D56BF81891535D2058EA2914220ED5FD392E8AE868DCA557

		F1C7C524013733F049D7F7B8173BEB
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	01764D6C70332A4CBBFF329CA405E08AFBFE8DBC1A7DE622E5BE1CA16835C8B3D6E0E6485B2FD8CCFF6BBEB6A6B99238B1345EEF84AB9946D79CDCF4F55B7A2A9488FD36E19D0AD8C1D56BF81891535D2058EA2914220ED5FD392E8AE868DCA557F1C7C524013733F049D7F7B8173BEB92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	df0utput	5BF99E01F038C368614644D41DD6C07A19F6C2B671E08910989E54790BE3FD71DCD8C1BE2761CE38B80923441 1E6FBEEDB9FA92B0DB2486D3C27165DFFA10F7F99843F7978638929199B1E2C1546008B9278148066BF3B88CF470E8244DB21322546018D314DE4E5EAD531B0528DBB
23	dfInput	005BF99E01F038C368614644D41DD6C07A19F6C2B671E08910989E54790BE3FD71DCD8C1BE2761CE38B80923441 1E6FBEEDB9FA92B0DB2486D3C27165DFFA10F7F99843F7978638929199B1E2C1546008B9278148066BF3B88CF470E8244DB2132546018D314DE4E5EAD531B0528DBB
24	df0utput	6CAEB1A0075BFA84FB399C02D429FD3643A3162629CE95C56BE42232C1B3B0986CA5E0ADD1F90C36B9892D20F7C72E08C9C13A23A82D7B80F1FC2AD04460A2B6192CB4C25CF9540969D7503DF3D9049994E4B45347A0483194FF339AE47566EDF7D2C7ED8856823996E8FC791917A6
25	reseed_counter	1
26	output2	E23FFC1E66485889E2B527DA492E1FA3C12AFBB1C1218CEBD3E2D332D0A616E0A2424BA439930A9A1F63B9034C30697BCED51DE82D00A28D107CE66ED100BFA4486ED6EF7BC40642F5385A2680D43EFB9BB343CD73DB4308389506094AA169F6
27	H	776EAD6B8C55F97F86D623F4EE0585C12F5A30881990EB7C127E73D7B3763021F4A6CC63300F6868BBD6F2CB1B863F0E
28	V	C8A84FA1F794BDED5C7FE0D6F200BDB05D99D8DC9BAF1ED6048276ABCD97AE0A497EA26BF95ADA6F7192506509AE29F7A560E34EB5DFC3EE2E23412E4401B2AD215E5FC82B565CB9599663580EA4C654818D50ED3F4AFFCCE2BA19D09F80AA14C3E52CAAC90CCFDB58B0F944F1E470
29	reseed_counter	2

5.2.4 SHA-512 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21

2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD4
6	dfInput	00560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD4
7	dfOutput	FAE0A1638A1CFCC6341B76625E49D0A292BF7E00C95CE06329913A21DE02E076C9C7C51D411A8D80FF42A3696AE66AFA91618A609F2356503AD354C869433C8C9603C75574CAA9FBA215EF4B54CF5244DCA5AEBD0AF4078891E3085C12101E679605FB37AC3A8418EEFDB631517727
8	V	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD4
9	C	FAE0A1638A1CFCC6341B76625E49D0A292BF7E00C95CE06329913A21DE02E076C9C7C51D411A8D80FF42A3696AE66AFA91618A609F2356503AD354C869433C8C9603C75574CAA9FBA215EF4B54CF5244DCA5AEBD0AF4078891E3085C12101E679605FB37AC3A8418EEFDB631517727
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	F886125A915AD892DC71EE95BA258D330D071DD4752C665EF33B1DD73E7A97D2A274C0D58F3B2E7D7A63AD0D7E6FCA38AF98C475979888CE4F51E9BFC790C7B1
13	V	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B3544DE34768D4760BB4A82815DC81E83F5AF4DC542428ADC47F0AD2882575C7A159ECFC54AB4933B5B428FD216D9BEF14DF932A98138C3B0ABF16234E0A7166285
14	output1	6E6E437B9AB5508CE0AABE544AF99A437B58CC7A53EA91EC18C28C2FD5D20669C7B330B12FD5D025AC40CCAB6056EB30B2B456F5E28AF74980BD00C960C0F7E70D030C1EC4C2EA0B70EE9E3BCE7F5FE8189941E2D6F1BC93DE9E0A101CBBC1F3826A00A659C856A3289BE91A6846A1C096328B4409B070D4564DCFC797300D57

15	H	CCD8AD3406CA6EB6E9679FC5E6930F2606D370DCE29D91B64776F89CA631BEAB2C0C1486B424670C62AEDB8F78F2A4992112EC43E678F625892A5F82163FF908
16	V	50EC5539A627FC27300FFE3B2A48B4C63088FA8CAE93BCAAA30169B701698C8909C0EFE423762CFFAF599CADFD81A10C484334F4B0F2C88424F478771AD65842B739E67A9D38A833C6370E48E308130FB87F8025C2966F2DD090AEAEC3A60581DB9BC056E8E155937B9218EEA7D2B5
17	reseed_counter	2
18	V	50EC5539A627FC27300FFE3B2A48B4C63088FA8CAE93BCAAA30169B701698C8909C0EFE423762CFFAF599CADFD81A10C484334F4B0F2C88424F478771AD65842B739E67A9D38A833C6370E48E308130FB87F8025C2966F2DD090AEAEC3A60581DB9BC056E8E155937B9218EEA7D2B5
19	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
20	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
21	dfInput	0150EC5539A627FC27300FFE3B2A48B4C63088FA8CAE93BCAAA30169B701698C8909C0EFE423762CFFAF599CADFD81A10C484334F4B0F2C88424F478771AD65842B739E67A9D38A833C6370E48E308130FB87F8025C2966F2DD090AEAEC3A60581DB9BC056E8E155937B9218EEA7D2B592BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8CEB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
22	dfOutput	E7E58C76687CC23780B31DD78083D055948B8842480C91E872A9BEB077B7DED3166AC8BB90792B4D6AF9EF1D50181E78C7A998845FDC181C21C3542E7D73EAAAFB16509100 19DD3C97A9494225A0C002C5D3F2B1DAD2C8266DA9CC4212AD0F0EF79F2F3A020933E1D7DC21AF0D2BAA
23	dfInput	00E7E58C76687CC23780B31DD78083D055948B8842480C91E872A9BEB077B7DED3166AC8BB90792B4D6AF9EF1D50181E78C7A998845FDC181C21C3542E7D73EAAAFB16509100 19DD3C97A9494225A0C002C5D3F2B1DAD2C8266DA9CC4212AD0F0EF79F2F3A020933E1D7DC21AF0D2BAA
24	dfOutput	F02A6FA25E8B3019867BDEB8667E21EDD69BDCCC7DD30623E43C54BDEB816C19FFAE794D77FE190404E45B8AB406A286D05E0DD25748A177F13014B928DDAB4A404BA7A384519F327BC7D6D54F37771B5C487B4E61225AE27E6F68F3C645976EE108332ECC5138DE7E0FF74E74E5A7
25	reseed_counter	1
26	output2	CAA3ED01A3E5B27EEC92E272EB4FC4753E8745D3566991714581 5EF72D980E2AB8BFB60A55F6EC2F29AAAA1DB58ED4D16033DEB0F203F3638ED6B530C70217B720542ADCAA92BDF11AF188ED98F65750578F34B64F831F3DD6F199814AD75EEF7E52EAF84AAB58DDBC28932DA914363EFA404B57E5EFF767E0518001BB3745E5
27	H	71B53CD3BDE84FA335254E8B070743B9FCAAA28CB1A87141AA6E517628598FB02AFFC492E60F335CAB2DF3D7444E2919118B22EAAF1ED24A246936EB3E714A87

28	V	D80FFC18C707F251072EFC8FE701F2436B27650EC5DF980C56E6136E63394AED 16194209087744516FDE4AA8041EC1714D447A149F745CC93841F3EEAD954FF1 E60484E62CDCBE1981C2963FCE67E74921E100E64B287FB41A0D0C7A271BBF8F 63CA4D17ED2CB6E4BF23043BF35BD9
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 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

5.3.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	CCF582F770A7808AB70EA6132A8304DB2D5F742F3B88D248DC2FF603E5B18997 F29CC0357DC9370D1129393FC66EF9B9330C63ED92E531DD
	output2	FEB974E9D3116B9DB4EE47943A9D3059C014242889C649D5BBFD6C72C5568EC5 9AE44D71A96A22E87C51A47319481BA7FFA4A88798E893F3

5.3.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	5FC15C6D61AFFDFBC5222A3FACEF17BA091C21E099911464EF6D6047BE290BAE 7A6C4278F6D49C970C14B83D302174BF7481FFFA865BD72475CCA8B8DA1A8D4C
	output2	F8DFB1F37DEC73434BC3AC414B9E5A7E6AA35AFC12E1CDCE498D55CDE282EFD3 3A0C811BF7FD0E019C150257BF23FDF15BBBE65FF78D5ACD90FA922AD6F05BD9

5.3.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	903AEB83C953468DEF4D56576C58BFC91D7CE5AC6C37716AADB1A55392F6845E BB89894465255D0BFA4BA061BDE6F6DBE994E8416D25D10FD86DEA0B74A9FDCB 4D425FFB9875E28BDB835A184DE38068BE41F2E5FA04C785BA32B564F8D3A76B
	output2	F5583836EBB04AA8E3C20F86BA541891EE14371BB21EC589EF08ECF10105FA66 85A121ED523ECFE80B0BF2DD94839357F77AA1DBFCC24C616D522349AD780DCA 510F07F35AB5BCA29CFA145D1898BB2B17B4BFBDF83852094EFC30E5796CD23F

5.3.4 SHA-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	6C690595CF3137B51307E928B14B9946F4B53825C6A7DD20E8B1121259A853BC 5F8E83A12668971A972BFDF4EF784D6EDF4734264300971DBE56D60A4C38A361 398C40C77EA4CFB97A36603600546E5ADC4FA4FEB1CFDF7C1543DE650378A078 D727C96B734ED9073A46046689F887042E681B70AB43477A93E5032659B99DE5
	output2	093812766ED02EEE0FB717EBA7CD99DFB3D928914127 73B1FF42B96F82421F51 46B580C65971FB33F101962BEBCA8B608FF7B5FFAEE3C69136B273528493B9CE FAF1F266219E8B98D3666881AEDC3D4008FE200986E8439DBB484E83C6FD60CD CC938E68D8E6A074E8D0318EA8FE820EED0C4D73436B673E09E79861C388CE21

5.4 시나리오 1-3 (개별화 문자열 사용, 추가 입력 미사용)

아래에서는 시나리오 1에서 개별화 문자열은 사용하고 추가 입력은 사용하지 않는 경우에 대한 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

5.4.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	79D7739CDA916F936B7874B26A8819F39B7E588D3122EB25CD577E78B0B24AC5 B3F71D2178E3712971A2182F5BAF3A7ED73039D65EFE8F04
	output2	AF2AD497BDEF7B5D4EDA18B39ABF7C6F35438D1F1C36E9F00378985BDC1D6DBC 819F4240807262DA18A83B9C7F14AFC34A4206A80586A0DE

5.4.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	04E722AE1186A8DBAD71354D9C1CE5437B4EC097EBDABA094ABEFB2288A8906C 93FA2647AD4A6533011F0FA4434C12EA6927F06D1B8630E434F75737C813A565
	output2	716314A5583254E822BFD8784141AB06B0CAD0CEFE37DC0BD4AAFD76DF49B77A 13DB0846B11D76D613D360055BBFED34B17B73B89D61F00F550E75C4AB882819

5.4.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	4B50EE127345485F6CEA8E1EC0EEDFB17EA6D483DF0E71F735E6BBDD51A0FA32 BE0571B3FCBFC68A7E83915F6DABDCBDD9D4C2B79464965D49D31822027AB8E2 DCF0CAD04995AA0CAEC4766A63B23DE87CA55884967EFC61EFAA74344D55C5C8
	output2	92875009624 1C98F5F27B9C0645287906E45AD7BE64EBF88484715F980867244 CC913050BCCADA3CA2E0AB14EE39A0B14C65B7D131D58EF83AA6904A1BDBDA67 A924FCF997687D5A0C51043F478F8C5BE2F6177B4B621E52D81DB982BF005713

5.4.4 SHA-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	C1A991899BFDD525748A9F00E94DC91B869D7DD7E0FC14A85E8AD5A18107937B 60E333F04866616031DE54146D7189DF3F0783ADEAFE292B2973D9820E54E308 C1DEE058DE58E35D3AB145A38D9960BD0221A3F57F99CE6844280D274135DB7F F3CE66DE53B29DA6F385480267366738E7C9D834E92E8816BC035D18B87A22A4
	output2	622E4508E0FCEEE8737A3DFAEE3EE19F2F2E1A639D7BE644ACEE9D358BF1664E B6D0187F5156A189E4221AF8BC6C366567FA436805BCD5AD6C73B8420760163E 55538EB18C1C7436468A37210E3A0DD542042DB418E5E7E30FCB5DE3377A4F87 67F205C0C0D7A6E2720B47B30EC2C82677FE9A05082F2281370B27A8E18BF0B2

5.5 시나리오 1-4 (개별화 문자열 미사용, 추가 입력 미사용)

아래에서는 시나리오 1에서 개별화 문자열과 추가 입력을 모두 사용하지 않는 경우에 대한 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

5.5.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	512785508725FC8C779C1055C20C5853FAC7BC250036DD1B76F2ADC650A760C4 4A3A78AB392A5FA461D5107F924F328599F9B49CC376040A
	output2	C586E6F9E6A48261F84C2F7E70A9993E6F2D6CCE09EC4236818E19C77CE168E2 7EFB70AB434BD919A97747C31FB4584058CF9615FC2A06FD

5.5.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	023B948B09B044DC5C0DFA84ADFF6684AC14D3E78DE38A0369F844CDEE378CD9 D6702C2FC4498407B25207C1AC88C12A48D38A4AE572EB9892811FCFABBC349F
	output2	61CAD09869BABA05D9FC5F8AF451F8A2751F94F40C58F1D1C7E1F15A85C6F668 D7F84D88053DCB8EC52C90336ACBA407955E37E92D9F7E45225FE76EEE130D0D

5.5.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	80545889E83DF70F3AD99E069639F888FFB6CB02284DE33E2EFA7CC5F78F86B6 0E36376F8E4C41CC02CD4DE79F103E93C0E17FDBC0398BA5C34ECCDAC89C670A 1B36E29ABC1A822934B89C9A6881FF25E8B8D3841ED3F314602A54D42B3A4A8B
	output2	AB5F40BFDC9A56ED54480FA7A1AE1E33595EC6ED0436B081186BD8885157E619 04223C487C7AAC8E751BB25FEF9E51D57D20BE05A0996A48B4E5A82D07B84A01 233F9F651A9875174DF35C9248DFC96CE7609E180FDA4C3EFEA039BCE7A49B86

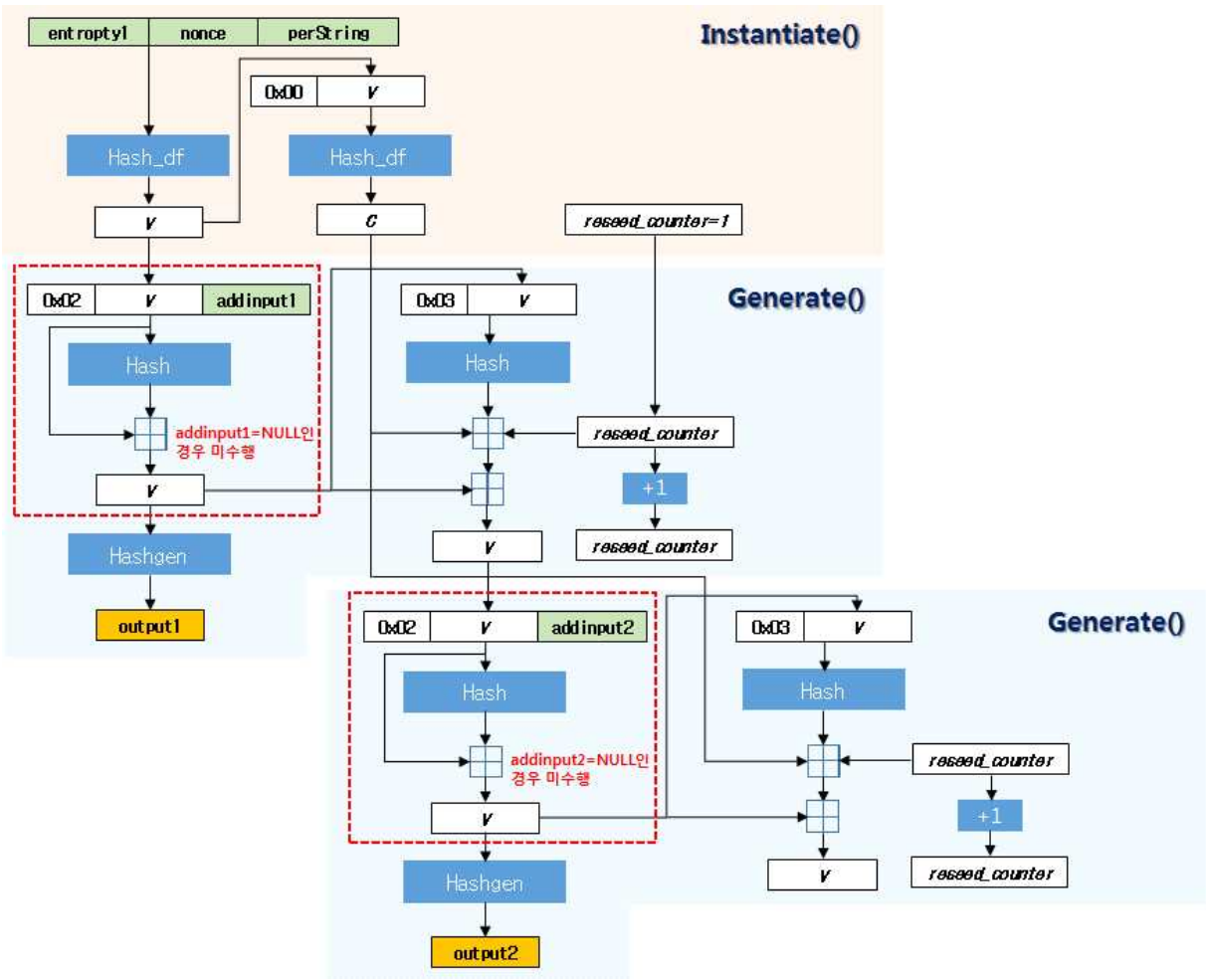
5.5.4 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	9EAC8910965B335B5E8CD3313434F5B93A5A663068E019BC4F9D9070B8631036 888170E2C6BEA23904BFC199B7A6A55E5E292A78647D30C5FE13795AFDA63C9C 385E64A402A495EF8FD82DA97ABFA8713AF41DAFCE76E560CB996F6B002AD7D2 95AFD26BE19462E808F0FCB88CD5D2642ADF4B932F69B0A903049 19C26D8E9EA
	output2	F14999734B31EC5A43EF8D3D8C4E5682BF864EFD4AF254804485688FD587264A ECE2D63FE008BDD117BCC6E6462F33925F450591D9F148BE67B3A6169B6A7906 D92C729C37C9E642BE13FE72ED6389EF62E63198B2E2284A3CBFAB8CC860CD55 38E5290FF28AEB7F68BE3B193E8F9066C5828F566EFEF72E76F8D0B6468B776A

6 시나리오 2 (예측내성을 지원하지 않고 갱신주기를 2로 설정)

6.1 개요

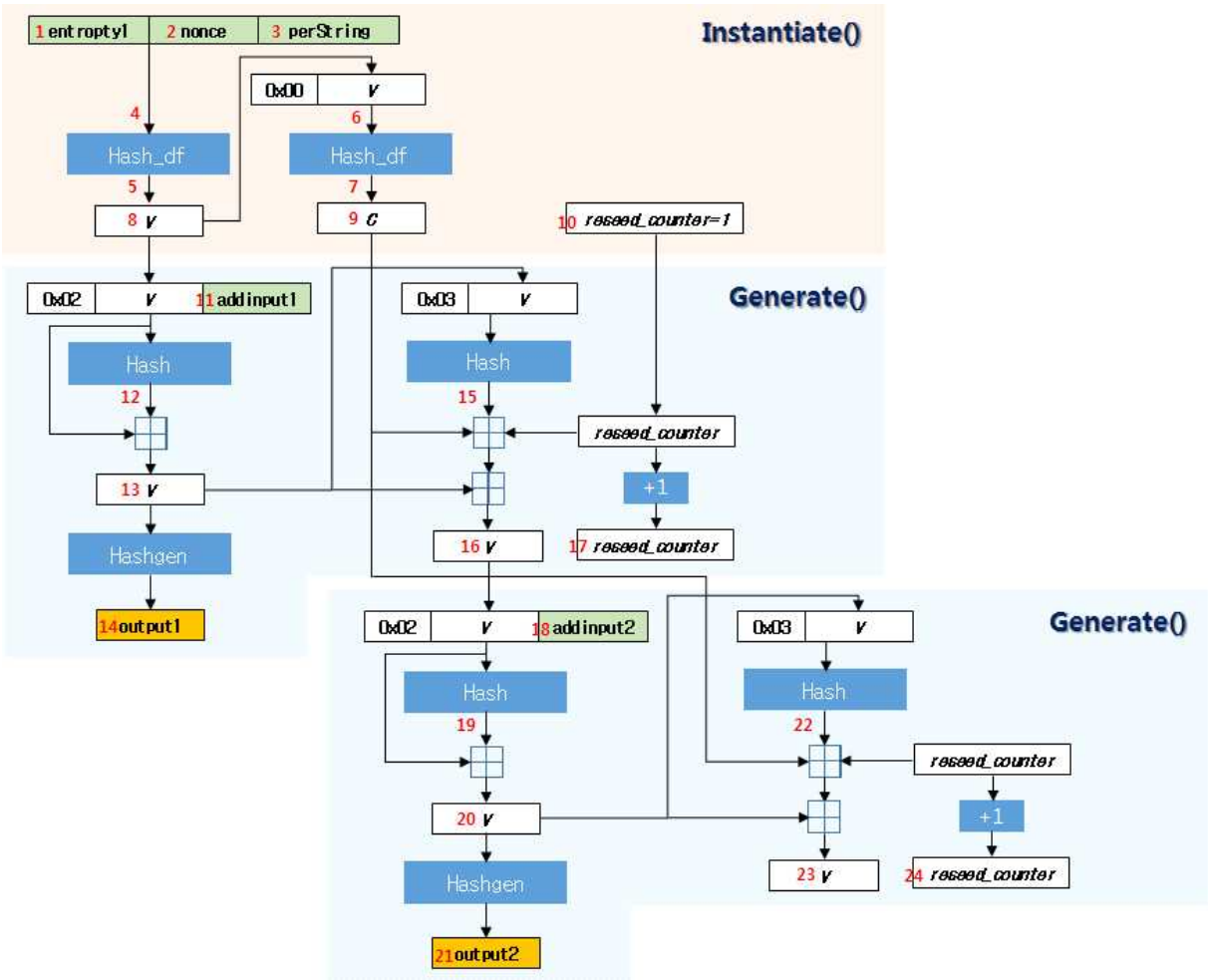
시나리오 2는 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 2로 설정할 경우의 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다. (그림 6-1)은 시나리오 2에 따른 Hash_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(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 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.



(그림 6-2) 단계별 참조 구현값 위치

6.2.1 SHA-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	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
6	dfInput	00E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
7	dfOutput	DB8C7A562E84DD05AC997876D9F525DA924729686868618E0FE7F04E5408210761707EE2C4B6E3E18D276A434DBA4F961360F72316281DEE
8	V	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
9	C	DB8C7A562E84DD05AC997876D9F525DA924729686868618E0FE7F04E5408210761707EE2C4B6E3E18D276A434DBA4F961360F72316281DEE
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	FAAB7AFFE93A64020803B5E50172C8740A17422FFF522770CFB9AA77
13	V	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4711D5926D5C43AB3CB869D20C56D9F5E085FFA7CE5780E9E23DDB687FC1
14	output1	FCD78232ED6A1AF0F3292FEAC467AA5DCB34FEE49A6276B0D57AA713F6EB998816F3A78EB8BA38ACB20D2BE1BD272A6347B90B639A80932B
15	H	629825803D7740C8196F8A2E38EFEA8BC9C1D40FBB8880D5E36117C8
16	V	C28F0B5EF2959C812C2622B7685285B0CD5B91BF3D4D1A4DE337608C32B3E3E292FC6347F87A66A00D35551723F1FD4FD35A36D4F1B578
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	ADF5F82B2BDFC2611F08AD522C10635C2B80A65D13460C142670F250
20	V	C28F0B5EF2959C812C2622B7685285B0CD5B91BF3D4D1A4DE337613A28AC0F0E72BEC4670127B8CC1D98B142A4985A6319664AFB62A7C8
21	output2	C4FF4EE1BF7CADD1AC7F66B0FFEED1378EFF403DF3DDB6CAD0D74F64ABBB90466D11177B1ECBF430E0C41A1FA9AAFBC56CFB4E0ABFD71AAD
22	H	CB00C8AABBED0B297737474ADBEA20B44772EF798B0DF25D6FD16239
23	V	9E1B85B5211A7986D8BF9B2E4247AB8B5FA2BB27A5AEA85DCB27B0593195C12BD048D0A2EF52E5352F23A8D7D1D76A01884FCB815C27F1
24	reseed_counter	3

6.2.2 SHA-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	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E 873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
6	dfInput	00866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA10 0E873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
7	df0utput	B627EC63298B14586333A30E8FCE253FCA97DF307830DE41F3CC48C41AD1E169 E68BAE253140B1A2C8CD4AF8C6B644CDBBD99C6BADF0CD
8	V	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E 873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
9	C	B627EC63298B14586333A30E8FCE253FCA97DF307830DE41F3CC48C41AD1E169 E68BAE253140B1A2C8CD4AF8C6B644CDBBD99C6BADF0CD
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	1FC204DD477216A2612E03D4BD18A45E7B95AB876CE5C4CCA27233953D7AAC0E
13	V	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E8E4BC9A4348D00B26F B542672398245DC66D7C241211699FBC99C76600723222
14	output1	DBEF6ECDEFE741B5EF1F34BA68384F6D5BBD7DA777429D96C74693A8513EB4BC BCC461B0C755B99493623CCDD31E3DE12281F5626BA83AC64594F51326C0068E
15	H	847777A53FC9C793831FFC547215C656799C6E9006B22682932B5175D3D736AD
16	V	3C8B2D67692AAB07B3DD2F4B4687E261011D8305BB050D54B70D9238719A275C BBCA69BADF2B65E2D2B7FF118A46671D80F2783FF7599D
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	EFEA3E74DFD8174A124F185A67EE198B938C552D58F098EA1AC93F2363942D38
20	V	3C8B2D67692AAB07B3DD2F4B4687E261011D8305BB050E44A14C071849B1716F 0AE2C422CD44F1765F0D2C6A7ADF51384A319BA38B86D5
21	output2	AAE98E6CEF9C06E195D3CF845E8D14697CAEEA5BF78DBBE5BCF8EF61C6115D38 468C76DEF53D6E9CEE8A007BB5ABBC545FCF883142737C7F3C73002FE6A55713
22	H	769CC3B3ED532C53E5811E38067E134CA33BFB18D9F93AB72FAF106913DDB791
23	V	F2B319CA92B5BF601710D259D65607A0CBB562363335ECFD31DC03C9B7AFA6BE 728CAA4E7C98EFBC63D5903D3AD04D35B51BA123172F35

24	reseed_counter	3

6.2.3 SHA-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	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7 F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74 D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA444 0C59237FB5FEB31B218AB18ECD701F
6	dfInput	00F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30B C7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A 74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4 440C59237FB5FEB31B218AB18ECD701F
7	dfOutput	840906E9246966BFD894747AD536AAB45E0804C785F29D18151EFF128515A80E F0D7ECCF74D44AC6A6AADFD59E5A49CC7936B6A4AA4CADEBE97B8A24E6801EFE A1DB67B49B74F4CE9BC49DFED0CF2C5C9556793B99B0D5D13770F94AFEF17844 08980223B8CCF6E40EE4528BA993D4
8	V	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7 F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74 D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA444 0C59237FB5FEB31B218AB18ECD701F
9	C	840906E9246966BFD894747AD536AAB45E0804C785F29D18151EFF128515A80E F0D7ECCF74D44AC6A6AADFD59E5A49CC7936B6A4AA4CADEBE97B8A24E6801EFE A1DB67B49B74F4CE9BC49DFED0CF2C5C9556793B99B0D5D13770F94AFEF17844 08980223B8CCF6E40EE4528BA993D4
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	765FA8D70A4FC126755AAC11869415A405260D48193F7D5F1530177BAA7105DD 44991BA705F2B296B60A11B44803838B
13	V	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7 F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0AEB 38CD0C5638B388EB379477AE09696C05C039CBA4B9CC6B4452BC8FCE5CA48188 A574CA85A8B149D12B9C65D6D0F3AA

14	output1	1E7809BD9BD6C557FFE5AAF7928B01C265CE644F7A7C79128A2BFCFE622F33FC A15D73EFA595F56537126F3F2B18A74C33E2788745321 16BDA44C563020FBA82 11364878B5261C29BE929334FBA9B399A1322EF295B221FD88D185C1FD0C81EA
15	H	AAAE54C2D6C8E25B080212E26BB71AC4BE0359E433CE9194E7AF0101CF0D46AB 8B43BAF87A9FB8F33B0F573F559CB46C
16	V	764D6C70332A4CBBFF329CA405E08AFBFE8DBC1A7DE622E5BE1CA16835C8B3D6 E0E6485B2FD8CCFF6BBEB6A6B99238B1345EEF84AB9946D79CDCF4F55B7A2A94 88FD36E19D0AD8C1D56BF81891535D2058EA2914220ED5FD392E8AE868DCA557 F1C7C524013733F049D7F7B8173BEB
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	A49EBD14D42AD736475C4D1B172A721F480EB478D249BDC85A555C01D0E88731 8FFBBA4116A3378B7D3C0E46B0FF63EE
20	V	764D6C70332A4CBBFF329CA405E08AFBFE8DBC1A7DE622E5BE1CA16835C8B3D6 E0E6485B2FD8CCFF6BBEB6A6B99238B1345EEF84AB9946D79CDCF4F55B7A2B39 27BA4BB5C7E20F0931B9132FBBC57C68679EA1E66BCC9E578E8A8CB95163D6E7 ED82063AA46EBF6D85E63E69169FD9
21	output2	48BCFBB6DF484B48CF145C6492C2F9E968D31E6A6D06B204C4BDA0228F00056F 4CD6ABDD06C0B0A500087AD9F187547EE2A70A4BF5E5752577E0438C6EEA25ED 4FC163E91A2332E1AD64D3D74D89ACD0627E0807BAF9A44C28867979440074A5
22	H	90D89833E33504292251E4E0B1370B9CA79425CCDC031810689D8FB092D29642 FB709BF9D3095AAEB7A25724977FC854
23	V	FA5673595793B37BD7C7111EDB1735B05C95C0E203D8BFFDD33BA07ABADE5BE5 D1BE352AA4AD17C61269967C57EC827DAD95A62955E5F4C386587F1A41FA4AC8 A22DE74D985B2CFA1F6291DFC3A0456C911AE7FE08958491638B369722EB9227 66B602316696650937 21B58C3FFC03
24	reseed_counter	3

6.2.4 SHA-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	df0utput	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC12 3FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A2

		46A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F271549 99E50BA12B27DDA2104B20DF859AD4
6	dfInput	00560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC 123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2 A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F2715 4999E50BA12B27DDA2104B20DF859AD4
7	dfOutput	FAE0A1638A1CFCC6341B76625E49D0A292BF7E00C95CE06329913A21DE02E076 C9C7C51D411A8D80FF42A3696AE66AFA91618A609F2356503AD354C869433C8C 9603C75574CAA9FBA215EF4B54CF5244DCA5AEBD0AF4078891E3085C12101E67 9605FB37AC3A8418EEFDB631517727
8	V	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC12 3FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A2 46A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F271549 99E50BA12B27DDA2104B20DF859AD4
9	C	FAE0A1638A1CFCC6341B76625E49D0A292BF7E00C95CE06329913A21DE02E076 C9C7C51D411A8D80FF42A3696AE66AFA91618A609F2356503AD354C869433C8C 9603C75574CAA9FBA215EF4B54CF5244DCA5AEBD0AF4078891E3085C12101E67 9605FB37AC3A8418EEFDB631517727
10	reseed_counter	1
11	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
12	w	F886125A915AD892DC71EE95BA258D330D071DD4752C665EF33B1DD73E7A97D2 A274C0D58F3B2E7D7A63AD0D7E6FCA38AF98C475979888CE4F51E9BFC790C7B1
13	V	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC12 3FF92AC6E25B9F7EB016F944929B3544DE34768D4760BB4A82815DC81E83F5AF 4DC542428ADC47F0AD2882575C7A159ECFC54AB4933B5B428FD216D9BEF14DF9 32A98138C3B0ABF16234E0A7166285
14	output1	6E6E437B9AB5508CE0AABE544AF99A437B58CC7A53EA91EC18C28C2FD5D20669 C7B330B12FD5D025AC40CCAB6056EB30B2B456F5E28AF74980BD00C960C0F7E7 0D030C1EC4C2EA0B70EE9E3BCE7F5FE8189941E2D6F1BC93DE9E0A101CBBC1F3 826A00A659C856A3289BE91A6846A1C096328B4409B070D4564DCFC797300D57
15	H	CCD8AD3406CA6EB6E9679FC5E6930F2606D370DCE29D91B64776F89CA631BEAB 2C0C1486B424670C62AEDB8F78F2A4992112EC43E678F625892A5F82163FF908
16	V	50EC5539A627FC27300FFE3B2A48B4C63088FA8CAE93BCAAA30169B701698C89 09C0EFE423762CFFAF599CADFD81A10C484334F4B0F2C88424F478771AD65842 B739E67A9D38A833C6370E48E308130FB87F8025C2966F2DD090AEAEC3A60581 DB9BC056E8E155937B9218EEA7D2B5
17	reseed_counter	2
18	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
19	w	FFC46AFF5F7C889B9CB65445F656DE4A50938754A14C60EE97BF236287D31A9C

		05503DD744091F2C390A4677F08D3096A29B7EFC6DAE0C5F28C071B00421B30A
20	V	50EC5539A627FC27300FFE3B2A48B4C63088FA8CAE93BCAAA30169B701698C89 09C0EFE423762CFFAF599CADFD81A20C0CAE34542D7B6420DB48BE6D71B4A293 4AC13B1BE99996CB855A70D0B622AF1508BD5769CBB59B66DAD7269F50D69C24 771ABCC496EDB4BC3C03C8F2C985BF
21	output2	4C35EB9678956C2CEA7931735D34E19A2857C28F4FE1B66561093BDF3D1419BC AF57381F6CFD1A8A9CC5ED990F159CD868F2BBE9C362C53E127688BC915F006D 2FE414476DDDF5139A3DDD87A99BA6C27A19C4DCB1BD6AC9329A433DE0B9E7DB 069A991D4033770B6D3B4DC010C1C5C681E26D7F329AB7B59369DD615975A3CD
22	H	F0F691E7F21B490A35CF563E95E068BCD6F0E3393D0C9288E3AEB468897E0B56 57592272B9A80C7F57B55A9DD686DA9DE575749A31CAA6A4098B727638A8D7B5
23	V	4BCCF69D3044F8ED642B749D88928568C348788D77F09D0DCC92A3D8DF6C6CFF D388B5016490BA80AE9C401768680DF794A1A6A6E7E7C4A6E57251CBBB609BF6 D1A83BAE6AF6C9AAD624C8A588FD57B13E8578E07EB6224722 14CCD1E9C15871 8295522E0DCEDCDEB673F55CC3D49D
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 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

6.3.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	CCF582F770A7808AB70EA6132A8304DB2D5F742F3B88D248DC2FF603E5B18997 F29CC0357DC9370D1129393FC66EF9B9330C63ED92E531DD
	output2	4FCA574BA7982B834097F7BA3DB935259A3179BB5A12EF560D936AE96407DC13 F45B770F4982F980959CE7E1E743886FE7C3716AC33784BE

6.3.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	5FC15C6D61AFFDFBC5222A3FACEF17BA091C21E099911464EF6D6047BE290BAE 7A6C4278F6D49C970C14B83D302174BF7481FFFA865BD72475CCA8B8DA1A8D4C
	output2	98B2F12FA93ECFC02B75E4839485D926E2EDBC676DEEC01E33C51CD4FE10C992 9C18F9D36E52CFB19585B3A3ED591D5DB023C04144E8ECBAC7F9231BF3F165B2

6.3.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	903AEB83C953468DEF4D56576C58BFC91D7CE5AC6C37716AADB1A55392F6845E BB89894465255D0BFA4BA061BDE6F6DBE994E8416D25D10FD86DEA0B74A9FDCB 4D425FFB9875E28BDB835A184DE38068BE41F2E5FA04C785BA32B564F8D3A76B
	output2	B55AF66F9A8CAB810429CEBAF3575C6B9799AA6AD501D17432F4E76D34DAE849 CB464DE84146A78D68C3E91AFB58B03572BB6BF61CC6DDC67ED0F34E9C83649A A4C80E573060BD8615D3310759A8C13A0E1E8CCE8B014ACC244AF79F2BE25A93

6.3.4 SHA-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	6C690595CF3137B51307E928B14B9946F4B53825C6A7DD20E8B1121259A853BC 5F8E83A12668971A972BFDF4EF784D6EDF4734264300971DBE56D60A4C38A361 398C40C77EA4CFB97A36603600546E5ADC4FA4FEB1CFDF7C1543DE650378A078 D727C96B734ED9073A46046689F887042E681B70AB43477A93E5032659B99DE5
	output2	8B1BD67D3D06A3A5D5A0FA8514A3C71A0B8F7050438C3A4386E7135A20605577 0CAB155BCC1FA87C61C440B42C882F4855E91FA785E5DF78AA79BCD06009A9FF E932C237DE058696B0544A7ACA48ED86CBCCE2CFF158F9F8AEBAD1F90E35A2B8 AA874B650570B376092F597747A23E5CECF77DDA0F5416801627512453B565BD

6.4 시나리오 2-3 (개별화 문자열 사용, 추가 입력 미사용)

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

6.4.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	79D7739CDA916F936B7874B26A8819F39B7E588D3122EB25CD577E78B0B24AC5 B3F71D2178E3712971A2182F5BAF3A7ED73039D65EFE8F04
	output2	35DE5221503EADA9D52190AA35A8EF9973D8AA4D4C220A1484AFC58422BA625F 323B5DDD2A7C0F2AB6FED5695429879F9B4109C475E67FB8

6.4.2 SHA-225 기반 Hash_DRBG의 참조 구현값

출력결과	output1	04E722AE1186A8DBAD71354D9C1CE5437B4EC097EBDABA094ABEFB2288A8906C 93FA2647AD4A6533011F0FA4434C12EA6927F06D1B8630E434F75737C813A565
	output2	750B17442938174A15734E65FB2E2B723A5FBE61B473DF5B37E1279140C59DE7 4D6A0A2ABBE5496429E7DE473D4FCCAB628D7BC7435ECE55BD6C6DA4874A850E

6.4.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	4B50EE127345485F6CEA8E1EC0EEDFB17EA6D483DF0E71F735E6BBDD51A0FA32 BE0571B3FCBFC68A7E83915F6DABDCBDD9D4C2B79464965D49D31822027AB8E2 DCF0CAD04995AA0CAEC4766A63B23DE87CA55884967EFC61EFAA74344D55C5C8
	output2	576CFB1457932DD0842A4323E2265458A66DDEC483EBD5A449092F2E5530D8D5 29C184DF0EB720C5EA6E50F88B6E742E302902C6AFF71CACDAC4D007C6FD33EE 4AF9F113EB4BDDD825327CEF38A5668A33E4E770B51177C77FA5BA4D41433930

6.4.4 SHA-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	C1A991899BFDD525748A9F00E94DC91B869D7DD7E0FC14A85E8AD5A18107937B 60E333F04866616031DE54146D7189DF3F0783ADEAFE292B2973D9820E54E308 C1DEE058DE58E35D3AB145A38D9960BD0221A3F57F99CE6844280D274135DB7F F3CE66DE53B29DA6F385480267366738E7C9D834E92E8816BC035D18B87A22A4
	output2	030D1D94F5B216DA3E9B122DB79E2C1CFE93EEECEA4130DCA6E8A19755ED611D 781500823651CFE472D13793B98E98070EB0C42C8174F0B88227FCE60CB168CF 4B5342352DF2536AE8053981B1DB79533C8E6739B159D0509AC3A6603F0425F8 1006EEAB6662B85F130A31EB8CCD62E387D074CC0519550E9095337D3AC8B492

6.5 시나리오 2-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

6.5.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	512785508725FC8C779C1055C20C5853FAC7BC250036DD1B76F2ADC650A760C4 4A3A78AB392A5FA461D5107F924F328599F9B49CC376040A
	output2	F32509D4203CC9C09EF698E445AB3BBBC36D0BF55D479E41B0A994F4F5EAFA00 A34B48F6F74BD70D7A3ED5BA78136DF0418CAC21C424D19F

6.5.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	023B948B09B044DC5C0DFA84ADFF6684AC14D3E78DE38A0369F844CDEE378CD9 D6702C2FC4498407B25207C1AC88C12A48D38A4AE572EB9892811FCFABBC349F
	output2	B07F50AA90AC5CD97009F3E6FAD7BE5BE1421C30AA7F31C2D56C18D4567D5275 F1DB4568423E2CF15804010ABF37AA5FAC2757ED4DFD3D22B03939493076AB9C

6.5.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	80545889E83DF70F3AD99E069639F888FFB6CB02284DE33E2EFA7CC5F78F86B6 0E36376F8E4C41CC02CD4DE79F103E93C0E17FDBC0398BA5C34ECCDAC89C670A 1B36E29ABC1A822934B89C9A6881FF25E8B8D3841ED3F314602A54D42B3A4A8B
	output2	CE9EEC96312B02470CF104B3D480D8EADF80BE7BBDAE952D04BE4788837BBB41 A497139EA853238231EA046D0123D851AECB7B499B2E5EA8932B28005E6B6F48 6F44338CFFC7C6CD978CAE3AB315D902321A19EE9A676D9A71FB0E22306A3344

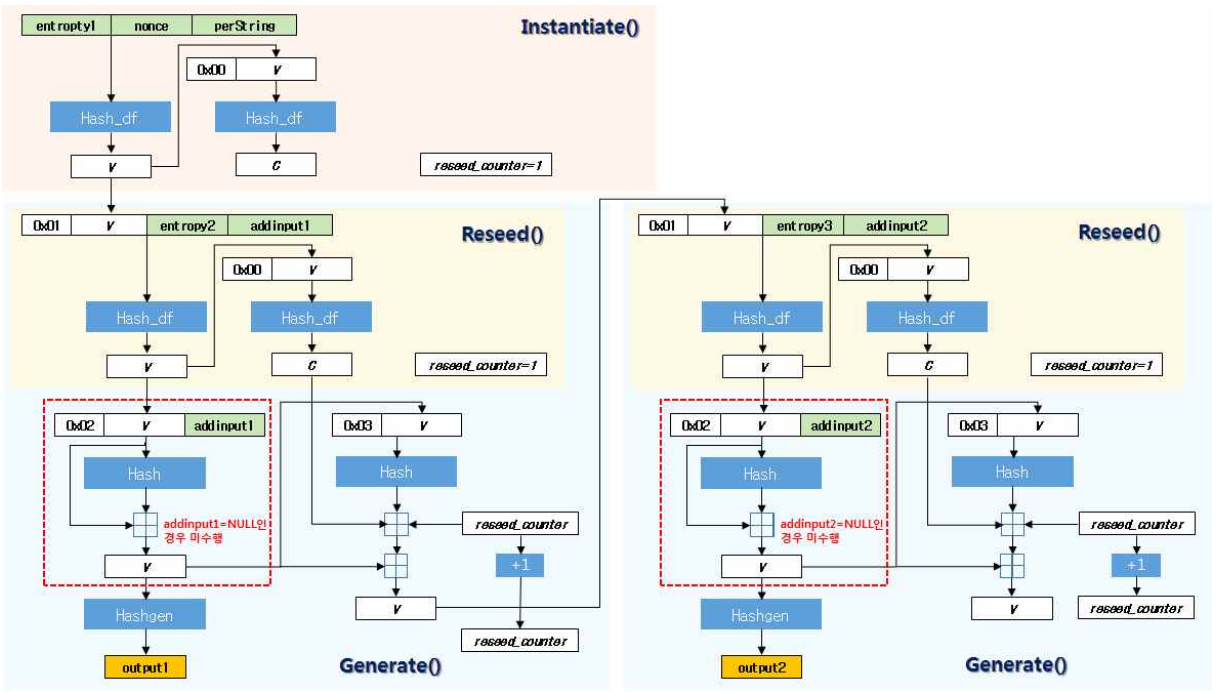
6.5.4 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	9EAC8910965B335B5E8CD3313434F5B93A5A663068E019BC4F9D9070B8631036 888170E2C6BEA23904BFC199B7A6A55E5E292A78647D30C5FE13795AFDA63C9C 385E64A402A495EF8FD82DA97ABFA8713AF41DAFCE76E560CB996F6B002AD7D2 95AFD26BE19462E808F0FCB88CD5D2642ADF4B932F69B0A903049 19C26D8E9EA
	output2	25BF514A83CCECEC5309E94CC44D5A8615D8E3259E64157A7B99ACC8026FC115 41E7FD0F942937B2382200CAB2E50A177B27CE348D57CA16B9AB8033B6BCF11F 2E7465308592CED7DE050DFFE99745C15FB1CE3FFBB28A40AFAC50E66BBB9F67 4F27262B2DDB25F8912AA3CDBF751EBE5D931DA9FF6F176E874D56C4671AAE22

7 시나리오 3 (예측내성 항상 지원)

7.1 개요

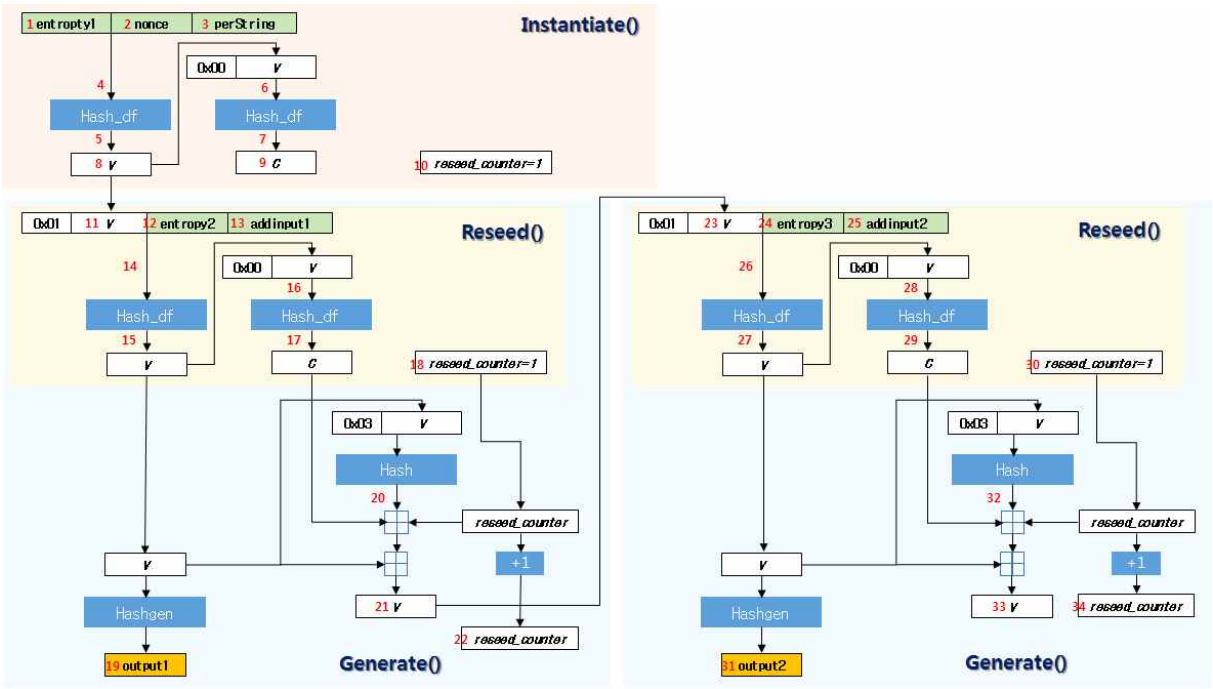
시나리오 3은 예측내성을 항상 지원하는 경우의 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다. (그림 7-1)은 시나리오 3에 따른 Hash_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 7-1) 예측내성을 항상 지원하는 Hash_DRBG 출력값 생성 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 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.



(그림 7-2) 단계별 참조 구현값 위치

7.2.1 SHA-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	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A 70D8B661CE5671D8831811F5908C278197BACD0BAED54A
6	dfInput	00E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C 5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
7	dfOutput	DB8C7A562E84DD05AC997876D9F525DA924729686861 8E0FE7F04E5408210761 707EE2C4B6E3E18D276A434DBA4F961360F72316281DEE
8	V	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A 70D8B661CE5671D8831811F5908C278197BACD0BAED54A

9	C	DB8C7A562E84DD05AC997876D9F525DA924729686868618E0FE7F04E5408210761707EE2C4B6E3E18D276A434DBA4F961360F72316281DEE
10	reseed_counter	1
11	V	E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01E7029108C410BF7B7F8CAA408E5D5FD63B146856D4EB8C3DFB4710DAE6F25C5A70D8B661CE5671D8831811F5908C278197BACD0BAED54A92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	df0utput	867EF75EF153C735868937D57029ACB9A106F493A03986EA4D0A73481AB950383C3F863BB9FE1EE271DAA537521F709614D51FAE5214C1
16	dfInput	00867EF75EF153C735868937D57029ACB9A106F493A03986EA4D0A73481AB950383C3F863BB9FE1EE271DAA537521F709614D51FAE5214C1
17	df0utput	33F60E5618A0467C37DF7172C12D0007E9CBF2D770614E934F6ADA5B3A8046F0C344F5CFDB5768AAAC3D8A33365778815252400C2E716A
18	reseed_counter	1
19	output1	5E207A4F3A5DE3B0E1291A8CB211E6DDC8E6171D5D2E36773FCA3BD3B37D23FDAF7EED8547F6EB023C589224834B710C0E5C40211B0A0143
20	H	7FD0EBDACBD70B9C6F75E96B3179CE720E0E0205B40DCBAA002E262E
21	V	BA7505B509F40DB1BE68A9483156ACC18AD2E76B109AD57D9C754E23262571F4D690187B0B3EF2BE97E6A1789678EECB74F30A8AAEAC5A
22	reseed_counter	2
23	V	BA7505B509F40DB1BE68A9483156ACC18AD2E76B109AD57D9C754E23262571F4D690187B0B3EF2BE97E6A1789678EECB74F30A8AAEAC5A
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01BA7505B509F40DB1BE68A9483156ACC18AD2E76B109AD57D9C754E23262571F4D690187B0B3EF2BE97E6A1789678EECB74F30A8AAEAC5AF148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	df0utput	0F526B22ABC759DDB83F9E6C4D211C7D50031A2AF63CA5C016EA1325D3B69D18057B4B9506BE8650BC210AF618BB20B9E359FE130143A1
28	dfInput	000F526B22ABC759DDB83F9E6C4D211C7D50031A2AF63CA5C016EA1325D3B69D18057B4B9506BE8650BC210AF618BB20B9E359FE130143A1
29	df0utput	3355EBFB9A7F649C8D34E83ABB412C3461DD5546AFA3624EE090CDD41D52938F53335CAE3035FBF8202EBDBB76442B3FA716EE74D4F1C5

30	reseed_counter	1
31	output2	B6A78201EE58F7CC968C957F00074EF81CE25E450CC2F56AE712F7F2DE959B71 183E5257FC67E4E2DB7E967304E235E186C0B3D05252E978
32	H	51A98CB34B84F2199B63E9B35D8102D54CF935E1CF34143208A0AE35
33	V	42A8571E4646BE7A457486A7086248B1B1E06F71A5E0080EF77AE14B9A95E3F2 DDA0C1DE9ADE35A65D529DFE88352DC8BE851E9076E39C
34	reseed_counter	2

7.2.2 SHA-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	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E 873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
6	dfInput	00866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA10 0E873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
7	df0utput	B627EC63298B14586333A30E8FCE253FCA97DF307830DE41F3CC48C41AD1E169 E68BAE253140B1A2C8CD4AF8C6B644CDBBD99C6BADF0CD
8	V	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E 873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
9	C	B627EC63298B14586333A30E8FCE253FCA97DF307830DE41F3CC48C41AD1E169 E68BAE253140B1A2C8CD4AF8C6B644CDBBD99C6BADF0CD
10	reseed_counter	1
11	V	866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA100E 873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F78614
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01866341043F9F96AF50A98C3CB6B9BD213685A3D542D42E6E89C4C6ED1AEA10 0E873E92667F7FFF4AD7D09CA52BA4D31A2793D0C2F7861492BAA7658C23A7EE 8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C6625B06B16AF81E7 13A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	df0utput	4AFB52BB86694E9B0D724462BF0F6E5241B74764EF2E566CE6990DF2B656E1C6 3C1BF2AF6A91AF9AF499DAB0F9462D35577CCEE96E1B85

16	dfInput	004AFB52BB86694E9B0D724462BF0F6E5241B74764EF2E566CE6990DF2B656E1C63C1BF2AF6A91AF9AF499DAB0F9462D35577CCEE96E1B85
17	df0utput	C8DC7F62BDDA37169DCE01B0E2C047F831A3DEB5E151E6F112F31448E9DA72B8CFFC4F61C1C968FAA47A36A2DB7294364C809060B65B58
18	reseed_counter	1
19	output1	7D05E202AF8B276890793B60CA6D98CD90FBC3A88676A50D34EDF000CC09C990F3888FBF22C6271D0C36FAAAEB279C35D55F889F7865EA4B1E1825789A2B114B
20	H	8D55DBF598A7148EF34496EAF6D7E63A5EB04C697A4FC65B267C0934ED740DA9
21	V	13D7D21E444385B1AB404613A1CFB64A735B261AD0803DEB4F6817D44745E37250AF2D08044152F449607ACE247F1C9220069437988487
22	reseed_counter	2
23	V	13D7D21E444385B1AB404613A1CFB64A735B261AD0803DEB4F6817D44745E37250AF2D08044152F449607ACE247F1C9220069437988487
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	0113D7D21E444385B1AB404613A1CFB64A735B261AD0803DEB4F6817D44745E37250AF2D08044152F449607ACE247F1C9220069437988487F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	df0utput	9EB2201ADE7161B5C7E5295A322B0EF0F309820C587CBE2A689970A568322778D661C56EB35E98DB813D4AEB7847BE38A7E5A8C54E5D10
28	dfInput	009EB2201ADE7161B5C7E5295A322B0EF0F309820C587CBE2A689970A568322778D661C56EB35E98DB813D4AEB7847BE38A7E5A8C54E5D10
29	df0utput	FE5E45A39B1C59FA8A627D8E4B6CB0CACA2DF858A4DF1294B6C1B1454BEA74E91B2FC4ED84C575E720CEE50CB7C6B7A6AD3ECE8F921C40
30	reseed_counter	1
31	output2	66F136FB284D547492F801DC0D6ECCCA554560A4610BC1E05A5648075514985AF997D9A0997025F67E1CDAC108895CFDAD3C66DC783E3EAD51038B0DCFDE29A1
32	H	4136F6DD1873211893F316B4A358FC0596B628ADBEEE04911443F5ED60F808BB
33	V	9D1065BE798DBBB05247A6E87D97BFBBBD377A64FD5BD1005651FF03273DB4F5E4A83EFF912014595834DDB71E1306F3991A64B5D8820C
34	reseed_counter	2

7.2.3 SHA-384 기반 Hash_DRBG의 참조 구현값

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

4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4440C59237FB5FEB31B218AB18ECD701F
6	dfInput	00F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4440C59237FB5FEB31B218AB18ECD701F
7	dfOutput	840906E9246966BFD894747AD536AAB45E0804C785F29D18151EFF128515A80EF0D7ECCF74D44AC6A6AADFD59E5A49CC7936B6A4AA4CADEBE97B8A24E6801EFEA1DB67B49B74F4CE9BC49DFED0CF2C5C9556793B99B0D5D13770F94AFEF1784408980223B8CCF6E40EE4528BA993D4
8	V	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4440C59237FB5FEB31B218AB18ECD701F
9	C	840906E9246966BFD894747AD536AAB45E0804C785F29D18151EFF128515A80EF0D7ECCF74D44AC6A6AADFD59E5A49CC7936B6A4AA4CADEBE97B8A24E6801EFEA1DB67B49B74F4CE9BC49DFED0CF2C5C9556793B99B0D5D13770F94AFEF1784408980223B8CCF6E40EE4528BA993D4
10	reseed_counter	1
11	V	F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4440C59237FB5FEB31B218AB18ECD701F
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01F24465870EC0E5FC269E282930A9E047A085B752F7F385CDA8FDA255B0B30BC7F00E5B8BBB048238C513D6D11B37EEE4BB2838E0014C98EBB3616AD074FA0A74D924354BE8F26275DCE866277553C8009A2C838B7A4F0C2F22A51423EB9EA4440C59237FB5FEB31B218AB18ECD701F92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150O7AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	dfOutput	9D80385E5624BD10D841221258358F07CCD60E159972A0A9F8D10D9F542250E7C4B6624E4537F8246DF022103EEFB73E4648CAD59DF74854AD8B40EDBE3FA5E40D42ED7584C2060181F56DEB80AAD01D931E4195E3BC15413A01A119A7D0FF8FE20CE8F844F88F88A2FDA88F2637A5

16	dfInput	009D80385E5624BD10D841221258358F07CCD60E159972A0A9F8D10D9F542250E7C4B6624E4537F8246DF022103EEFB73E4648CAD59DF74854AD8B40EDBE3FA5E40D42ED7584C2060181F56DEB80AAD01D931E4195E3BC15413A01A119A7D0FF8FE20CE8F844F88F88A2FDA88F2637A5
17	dfOutput	2BF282F7FB5CBA02FEB8AFD4B4EEDE2D239037551D45EAFEF543A89BDD403B3ED81E1FEDAD0A8A741F18F54CFE4D5440795B67ABF3156A135B34AF6814775A9C4045A2AF21C723AECDD9DF5B9AA5DA329DF0E2263FF8ECE011680686E99E26144E80CE3D321351D2A4E6ADF9EE2235
18	reseed_counter	1
19	output1	21AFE24A877E07105CA637235F94924EA06AA66CC509144F61CBB413D54DF07334AE28AD867B059BDF2740DEFA22CC998042CF09D835092EAEFDA8CB71EDB813D7C4380BF13C90D96B86B2C5C3C2BAB7F13F03F7D678E5387055AE132EDDFC52
20	H	726504E5DC0F2F61F7B01B7725DCFFEFB02492AB51FE471EDF91B9729199 78D5BA55D6E0B331F7B5BEDFA1A0BEB2FD4F
21	V	C972BB56518177 13D6F9D1E70D246D34F066456AB6B88BA8EE14B63B31628C269CD4823BF24282988D09175D3D3D0B7EBFA43281910CB26808BFF055D2B700F2B28D7600B5B88BA7FFEAC46CF8509A0055A1CF0E21FC2100DD231A322AE7FB5E866497E8A903971A2785F747C7572A
22	reseed_counter	2
23	V	C972BB56518177 13D6F9D1E70D246D34F066456AB6B88BA8EE14B63B31628C269CD4823BF24282988D09175D3D3D0B7EBFA43281910CB26808BFF055D2B700F2B28D7600B5B88BA7FFEAC46CF8509A0055A1CF0E21FC2100DD231A322AE7FB5E866497E8A903971A2785F747C7572A
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	01C972BB56518177 13D6F9D1E70D246D34F066456AB6B88BA8EE14B63B31628C269CD4823BF24282988D09175D3D3D0B7EBFA43281910CB26808BFF055D2B700F2B28D7600B5B88BA7FFEAC46CF8509A0055A1CF0E21FC2100DD231A322AE7FB5E866497E8A903971A2785F747C7572AF148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	dfOutput	8950414253F2534FB6B7888003D8446A44FB50B9E5DC607230640CA53379ECC9CA3106BEE0EA301374029E50F3914735CFCE493A8C4B1F1FC7585ED7E97DA7BF37AF29D377D2E253CF2E25AF3C4F03029D2B9228C48075486AB531DDBB5CD3A2A77C09B656AF9A8EA2D6D0CCEC33C4
28	dfInput	008950414253F2534FB6B7888003D8446A44FB50B9E5DC607230640CA53379ECC9CA3106BEE0EA301374029E50F3914735CFCE493A8C4B1F1FC7585ED7E97DA7BF37AF29D377D2E253CF2E25AF3C4F03029D2B9228C48075486AB531DDBB5CD3A2A77C09B656AF9A8EA2D6D0CCEC33C4
29	dfOutput	777594B183F4A709AA39B385657ABD99996BEC5D2182940EBD5A5C6630C0245B

		5A2068A71F2066F4DFBBE7BB64CB95F481D2F585C40CFAE6664C3D185FD2C697B0D5F9020284DB9D16BDAC063B85B10AA21A446E577348CE17093B76E4CA64E301887E8146CCBBA41098A3138B4347
30	reseed_counter	1
31	output2	75C72B7677702FAA7C7246D915B88825AC575AD7B98E6B8EDF6D36870FC9B91640897667A456208974B0A55DD7A54EF1C4FC28AA354AA335D3C13533A2B525A84EA871639A500B4BC63FE188A7681385AAB2E3041B3D84F4B1E4D15615ADCF20
32	H	1025ED81B6833C3D4246E7AA5706665235FE0628F3039C4680C841DAF77AFCBE1339177C469F9D5745CC96529E70EFD4
33	V	00C5D5F3D7E6FA5960F13C0569530203DE673D17075EF480EDBE690B643A112524516F66000A970853BE860C585CDD2A51A13EC050581A062DA49BF049506E670E72A48BFD93FB332CD37C0C7E3B06433D4BFF8A1F9004974A00484C1B23F698E21C047E3D19AD788005C67EE866E0
34	reseed_counter	2

7.2.4 SHA-512 기반 Hash_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	dfInput	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21BE1FC13D9266E5280C87112E955995F3A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
5	dfOutput	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD4
6	dfInput	00560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F271549999E50BA12B27DDA2104B20DF859AD4
7	dfOutput	FAE0A1638A1CFCC6341B76625E49D0A292BF7E00C95CE06329913A21DE02E076C9C7C51D411A8D80FF42A3696AE66AFA91618A609F2356503AD354C869433C8C9603C75574CAA9FBA215EF4B54CF5244DCA5AEBD0AF4078891E3085C12101E679605FB37AC3A8418EEFDB631517727
8	V	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD4

9	C	FAE0A1638A1CFCC6341B76625E49D0A292BF7E00C95CE06329913A21DE02E076C9C7C51D411A8D80FF42A3696AE66AFA91618A609F2356503AD354C869433C8C9603C75574CAA9FBA215EF4B54CF5244DCA5AEBD0AF4078891E3085C12101E679605FB37AC3A8418EEFDB631517727
10	reseed_counter	1
11	V	560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD4
12	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
13	addInput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
14	dfInput	01560BB3D61C0AFF60FBF487D8CBFEE4239DC97C8BE536DC4779702F952366AC123FF92AC6E25B9F7EB016F944929B344C58221BFBEC88286E1092C80DF8F6C2A246A76DCD5E75E8FD720AAB18E1E242FC5B047525580CDDC82C25095B4F27154999E50BA12B27DDA2104B20DF859AD492BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
15	dfOutput	5587AB000CA15C5898A9211F741BB09B82D5F7FC0AD72F8F84AC337308245E04FC1F32F228C9A219BBD7226D8B8BFE12A7DC0BD582F13D2C1AE7AAE8129C34BA26D69B23F0820F37107931F76BC72AAEFD15791ADADEDB95FDD32B6A21B403C06BD5EAAD8F6ED4677D3C571DE867D2
16	dfInput	005587AB000CA15C5898A9211F741BB09B82D5F7FC0AD72F8F84AC337308245E04FC1F32F228C9A219BBD7226D8B8BFE12A7DC0BD582F13D2C1AE7AAE8129C34BA26D69B23F0820F37107931F76BC72AAEFD15791ADADEDB95FDD32B6A21B403C06BD5EAAD8F6ED4677D3C571DE867D2
17	dfOutput	FA7E6E53D4DAAEA3DFBA645DE1DAE6BC460C44E49435281EE3E986FEB61C3031258B24C9A23C34BE2FC4965FB99CE0973371A3B7E2BEF061B7D9EC468E08794F85DA20F266522E87C02F9B702CAB8AAF64B04B9E3C3960DCBF95414016B3DB39AB5FB114FCF7599229A73DF61D972C
18	reseed_counter	1
19	output1	247AAC36E9E49EFD53531C4FE0C66707962D6C3DBC9C6369A6EFE1A3265D11C9A9E1934D32CF39FFF7DC01FA0B7DC0CE20B6B2D1BB50414FD723333779384B359E0C32C7C3BD89269DDE4F3DF2444D605A8CC75A3E65B5B868EC3048F00887BC24221D8D21DC256EC4223FB40B654285759316FF82FF46B8E880DCCF8EA31CB0
20	H	1C1491C2DD19EFDF7D7C5B2DEB77C31D840039DDFB1BF8CECA8A2CB05276A6A25CED7A4075BBEC8D4B36E26C5BC78C8F279498D644279172AD6B6CC8569569C5
21	V	50061953E17C0AFC7863857D55F69757C8E23CE09F0C57AE6895BA71BE408E3621AA57BBCB05D6D7EB9BB8CD4528DEC5EFDF726A7FA00D0B4F1CC51A1867CB8DACEA9A1172CD0C895AD57DBA0F1957BB4F40052ED304C9BDF44AD905FFF46E21ABCE7206B3F7A0A712505D6A9B68C4

22	reseed_counter	2
23	V	FA7E6E53D4DAAEA3DFBA645DE1DAE6BC460C44E49435281EE3E986FEB61C3031258B24C9A23C34BE2FC4965FB99CE0973371A3B7E2BEF061B7D9EC468E08794F85DA20F266522E87C02F9B702CAB8AAF64B04B9E3C3960DCBF95414016B3DB39AB5FB114FCF7599229A73DF61D972C
24	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
25	addInput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
26	dfInput	0150061953E17C0AFC7863857D55F69757C8E23CE09F0C57AE6895BA71BE408E3621AA57BBCB05D6D7EB9BB8CD4528DEC5EFDF726A7FA00D0B4F1CC51A1867CB8DACEA9A1172CD0C895AD57DBA0F1957BB4F40052ED304C9BDF44AD905FFF46E21ABCE7206B3F7A0A712505D6A9B68C4F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
27	df0utput	A587404B9A66E5BDF66DC4B6FC2064363304913089 9ADEDD633640354C35D4747139B41EE4B971CC916E3A755A8E7C010CB8D1C4F0F0F05D70090691574FA536445A0BC4AD5CFA6F42DF08138411728F831E095ACB7F1DEB0030B3397654296F40A82DE856BF81500DA73A7F633AA7
28	dfInput	00A587404B9A66E5BDF66DC4B6FC2064363304913089 9ADEDD633640354C35D4747139B41EE4B971CC916E3A755A8E7C010CB8D1C4F0F0F05D70090691574FA536445A0BC4AD5CFA6F42DF08138411728F831E095ACB7F1DEB0030B3397654296F40A82DE856BF81500DA73A7F633AA7
29	df0utput	4D89E15CEB3569745DBA82C3FFA4F087CFA834E6893A1E53CA8A81EC072047BCC31DA6CE0129710717DE1F2A7B7D4063655632F2D23FF776946ACA9F449612C033B5421D1E19D12C41B4D6A7F73348B8D22A9051E18BDF427F82D4E3214A89DF7CFFA6C625276CED44E0FE90492CFB
30	reseed_counter	1
31	output2	954B0EE05D5BF49AB364D5263B025D3466971D8E8BBC639177214C8EFB5CF76DDC7C998E5D243659D677131E5D0AF31ADEE5EE31AB47E731F0766872F08E832FAE1268D9B7C25704F4ABAF27866E02144AD0A96C50C370C22B35FAC39D15D458800C42E5C1979F379842C478C07766346BDC39467F467F89EF3CAE9838893B26
32	H	4B2159C52E592D44CB12256ED94F7A3F6C20796CE6122DD73993C17FC3BCEF8DDECB597E9E8D3771F689921AFB5CB6D9BE0DD67A59B8B7852433F152638B5CE8
33	V	F31121A8859C4F325428477AFBC554BE02ACC61712D4FD312DC0C22153561C3134575AECE5E2E2D3A94C599FD60BBCAF9368C9E61C5E2C9F16994009EB5FF7629888BAC7DDA4A2D518555E7F3834492720A2184B3A426F240945A317F4558D0CCB7E4F08349E736186798B7337C48B
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 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

7.3.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	0052590D04395BC22A83BDA10942C8927943E41FE634BC4472BC52F08ADB2CCC 5C420564F87E28B675B73F5FA8D374F3A3B3093151D8FB4D
	output2	92F6A3DF252ADB2D5A1D09CD27B6174E406E1407533FA12A39D41A1799F1C6DA CF8ABB5CF85D8C4B7BE0D9E754ECEADF3649677949FDC939

7.3.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	07FC09860EF3B150F5362B45FA1CF6C90B7D5BD06D1BF1245C75FB0D853DCFFF 8423F5FCE3901046776C75646223D1A1E57309D01D9821203B244BD10F901AFC
	output2	A00977F40B580644FDA77023AF690E7FBF643642CBF42C75DDB7BE677709A3C9 3096E16260E9EC1FEBAB2B07671A080FDCC1A3FDF487E13460647C3EF000E28A

7.3.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	D102ACB9CBF34DDBF4167A4020A12EBE636BC48A11C80DE49F0FC365AF505730 9B72550CCD227838CA4B07926CEE05B8FE56603CA90E03D66D13B2AF4F0FF788 C5F8FC5204500A425782E28BE788487ADA6F8C4CF0991E0835456E84F86EE4C2
	output2	A006EB3701D968240532426872F614B475057C0715917712C23F84A56293A2 9CA4FF951E0A859F6F31C67DB33EC6CAD444F4CFDBBEA8C0FCA58B0B7646DDA4 CE66F30B673EF97BD90DEF060A60423747993A92D34C0BA03BFB0CC09328B927

7.3.4 SHA-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	B39F9D62D43F8FB48EAFBFBDAFDB66091EA33739255B01C69C4828A41A229357 9A52827EE2BEB4186BD34C644DD7958BD3A55D75D36EA90CE12A1C963F385A00 63240F7E9C9C4A86509DC0C235A05574D4AFD5CF61DCDA5779AE38020CD9D946 94B66241453860C77A75F163A637BD185AE7EECE2F2ACD05A66BC2DBBCAA64A0
	output2	26AA9CC9748FBDD21C7B242DF3D0F50BC124999F30999C2239133BA210BE2679 D80B52C23946521F9509490730C82B124AE4559F15BE029F99E0FCD7315E6076 2EC798DA8B87AC5707987AD0F7BA4B97EF00F1453AAFE013954ECE405A6EA718 F0C8DBF4CD9553B33D95676D4ABADABD3F3B662BB47B8C07815B5134ED22A73F

7.4 시나리오 3-3 (개별화 문자열 사용, 추가 입력 미사용)

아래에서는 시나리오 3에서 개별화 문자열은 사용하고 추가 입력은 사용하지 않는 경우에 대한 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

7.4.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	AF25073AA427AB6868690E927F333D7056842EEBF5DE0F30D6331ED3DB3744C9 D43B15604A17DFB0524A6679190827418FB80B3C017E6E55
	output2	E985E2BE5A637CD4F4318483C06343708A5ECDE7604EC3C4083B1071430AC441 279D1C55F45B47D545DDDB595E5F4F0A62C23D31379FD9DE

7.4.2 SHA-225 기반 Hash_DRBG의 참조 구현값

출력결과	output1	BAD1941636023260AEE986FC8DDD784CF435E678A5F23960E518AE388252C297 2CE4EFCDEFFD20B1A2211B3EA1A2C803437E1C7C6781FD39C47E6CDFE548DE0E
	output2	988B1CFCC7C3465C00D98DA38F1EAA0750F733EF30C668444F26FD965A69C3C2 54CCA2E427BCB6B9F81403368B42F53353D882D6AA8FAD8E9AD7FBE88E1F83F2

7.4.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	449B9B5CD39EFFC63D6464C2BC776ACDBEA79D77BB886771AC7CDA922A4EFE2F 72B7A48B3CFEA3FFC8DBB6BE0C777A2D3823ECC5B94C972032FC63ABF30ABB28 0550C528E2DBAD2F96C00C82CD5C8218BFF88DA33917C1553AF514EB5307ABF2
	output2	E202E295E5CEAFFE15014C5EAF308B842F2ADAF84DF86395A960A22872DC173F 4AB151ED5EC8C57DA1CE5D397741F2478DD2BA100815A0DE6714B13741F70B21 9AB2718705F54BA993A17D9373B99A858A0157D5AAB078E492EB133B27FF702C

7.4.4 SHA-512 기반 Hash_DRBG의 참조 구현값

출력결과	output1	6D2781CA19FFDD25B2120126E4A42111B00F0AEDA9541ECE6C91AED23347C61D D4A29DFC6DD9DB1A0E67DB4CF7A8034E80C58E06C52D1F7A6674BB0A95FFFFCE 65EC293E3DEBBBC8363F6D7943777B6AFCFF7F4173361D5A5B62DFE79237FBB8 85243741BA395FE9AD732D02730667DC3F59524FBDE21DD105EFADF7CC181FC7
	output2	E0745F2488115C0990F9A10BF9026AF07E1A05BD93833167BFA7A0F1C4357CA3 178602E8D488F6C47EB0F229C5127608FB09323114A73AFBB607DA61E22F9305 7C57A9F5C6610696456FA5304CE0D215A95CBACFFF1ADD58399CD1BE43DCC271 632B58B37F8CF9D407985DFAE5536E2BF3360D0CF90B3838F59459D09E904591

7.5 시나리오 3-4 (개별화 문자열 미사용, 추가 입력 미사용)

아래에서는 시나리오 3에서 개별화 문자열과 추가 입력을 모두 사용하지 않는 경우에 대한 SHA-2 기반 Hash_DRBG 참조 구현값을 제시한다.

7.5.1 SHA-224 기반 Hash_DRBG의 참조 구현값

출력결과	output1	DBA74BE8021A0249A389996EC188BED5A0F608D5B771D4BFDF22BC6166607AC0 FAC43D0F7DA21BF1EABF829B04315E74C97B5F2FCD861114
	output2	BF0CAB7E12F5443218374CA9CF4B27DCC674C2F1FC59773950880E05F01FB946 BF2B1FC66603054430BF6D346C3600FBEAFBAB2E04DF3E11

7.5.2 SHA-256 기반 Hash_DRBG의 참조 구현값

출력결과	output1	B428FF753A23DCA15C6277777C1827F126933B97EB4986DB54B8D596BF147381 7A3C9C8391CE1BDF0CA2EDDC6697D62F34B9EC9B3271AE0F5E7C096C092DB017
	output2	24EB6EF2402E02F3832348CF718B192D32C4FBCB98F19F87182E68FA3A159AE9 DCAF2BC3B11BEA9BAA54F602EAC7931B32CB73C0B9B2E8D9972BD6D6479E8478

7.5.3 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	3E92A9330C7BF2A801554386EBEC52EF613E48FA98D8F127F3D0D4978A623499 358D6E0386E51EEFE46B3B7F6297DAE1E2BD21AC2D17A0C636760C453E3174BF CEA3C2F7F9D1ED2981752894BF8D41D6C38D12E099D0DE236B8A36EB3346059E
	output2	334A2D85E5BBAED5581E21FC14CFA48D18AB8E368FD38397DECCF52CB9BE2B35 E867B63CB538A63AF9EB27C196FC78A27F332FAB6B57B18B90695CC75F1FAD10 9B761661FA683C2D131E8833B700C3C5678E1A4121CDAEB275AEE9DA04E78BE0

7.5.4 SHA-384 기반 Hash_DRBG의 참조 구현값

출력결과	output1	8CC0AFFF0C0A92CD39DEBF25AEA0B7A398C1B9D1EF9CACE268F66C9BFDB82F1E 25FDE596766F9152E69C03F98269F82D07D43E8ACF266FB3DE041B97CEEDC813 460FF22C6D5B922AA976B07DD9C9D3E549BAAAA2B2C55EC0FC6FE0E5AE000AD3 98F349856728FFD01D30EC85CEC5665FF1EAA08830D582C1A595C816A586EA74
	output2	AB5840458CC0353792E7BAFA9699CF2DFC0F4E389990C7908B982E23B4473DE0 3487F884D34C70E6FF261F33858AFC53942C10333AA92B9BEFDD30A02343F361 E3E965603A47CC04EA74144729C58FA5109F0E8F125F6CC84ABA5CF62101EC98 0136D490136554428B9BBE044EFE2FB842A825B6C93AB7C809B9B43756AFFA0A

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 TTAK.KO-12.0xxx-Part1

이 표준에서 제시하는 SHA-2를 사용하는 경우의 참조구현값에 대한 구성, 용어 정의 및 약어를 제시하는 '제1부 일반' 표준임

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

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

[2] NIST FIPS PUB 180-4, “Secure Hash Standard (SHS)”, 2015. 8.

[3] ISO/IEC 10118-3, “Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions”, 2004.

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

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.xx	제정 TTAK.KO-12.0xxx-Part1	-	정보보호기반 (PG501)