TTA Standard

정보통신단체표준(국문표준)

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

HMAC 기반 결정론적 난수발생기 - 제2부: 해시 함수 SHA-2

Deterministic Random Bit Generator based on HMAC - 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 사용하는 HMAC 기반의 DRBG 메커니즘 HMAC_DRBG의 참조 구현값을 제시하여, HMAC_DRBG의 구현 정확성을 확인할 수 있도록 한다.

2 주요 내용 요약

이 표준은 HMAC_DRBG 운용을 위해 고려할 수 있는 다양한 선택 요소(예측내성 활성화 여부, 시드별 출력 값 생성 횟수(reseed_interval), 개별화 문자열 입력 여부, 추가 입력 사용 여부)를 반영하여, SHA-2를 사용하는 HMAC_DRBG의 참조 구현값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 제1부 일반에 규정된 DRBG 메커니즘인 HMAC_DRBG의 기반 함수인 HMAC에 ISO/IEC 10118-3에 규정된 해시 함수 SHA-2를 적용한 결과로, HMAC_DRBG와 HMAC, 그리고 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, HMAC_DRBG, used as a HMAC function based on message authentication code HMAC using SHA-2 about implementation conformance.

2 Summary

The standard specifies the test vectors of HMAC_DRBG used as HMAC(SHA-2) about implementation conformance. The standard reflects the various options (prediction resistance, reseed interval, personlization string, additional input) that can be considered for HMAC_DRBG operation.

3 Comparison to Reference Standards

3.1 Relationship to Reference Standards

The test vectors in this standard are result of applying the HMAC(SHA-2) specified in 10118-3 as the HMAC based on HMAC_DRBG, the DRBG mechanism specified in Part 1: General.
And, HMAC_DRBG and HMAC(SHA-2) conform to the specifications of each standard.

목 차

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

1 적용 범위

이 표준은 해시 기반 메시지 인증 코드 HMAC(SHA-2)을 기반으로 동작하는 DRBG 메커니즘 HMAC_DRBG의 참조 구현값을 제시한다. HMAC_DRBG는 운용을 위한 다양한 선택 요소가 존재한다. 참조 구현값 생성을 위해 고려한 선택 요소는 다음과 같다.

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

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

상태갱신 주기의 설정과 예측내성 지원 여부에 따른 리씨드 함수의 호출을 고려한 상세 시험 시나리오와 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 1-1> HMAC_DRBG 난수발생기 입력값 정보

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

- DRBG의 기반 해시 함수 알고리즘에 상관없이 <표 1-1>에 정의된 입력값을 사용한다. 단, DRBG 출력값의 비트 길이(requested_no_of_bits)는 해시 함수 알고리즘의 출력 길이의 2배로 설정한다. 예를 들어, 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 1-2>와 같다.

<표 1-2> 부가 입력 정보 설정에 따른 시험 분류

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

2 인용 표준

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

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

- FIPS PUB 180-4, “Secure HMAC Standard(SHS)”, 2015. 8.

3 용어 정의

- 해당없음

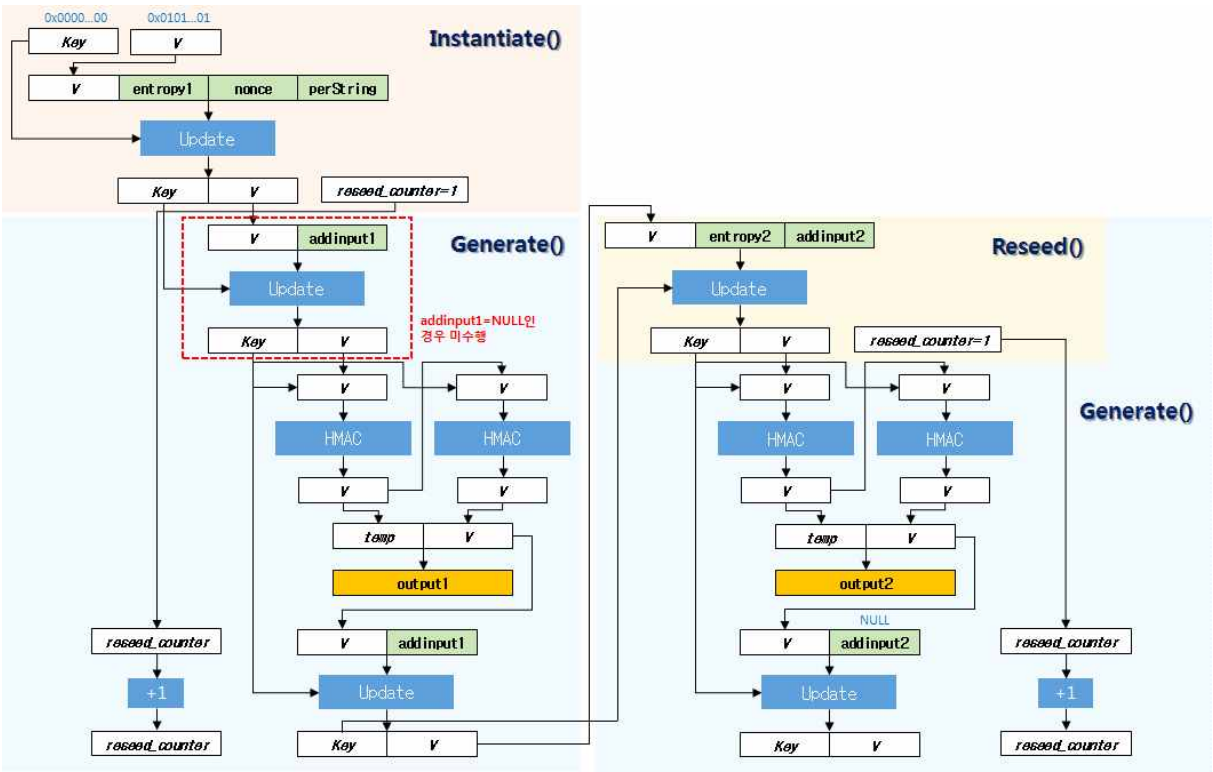
4 약어

- 해당없음

5 시나리오 1 (예측내성을 지원하지 않고 갱신주기를 1로 설정)

5.1 개요

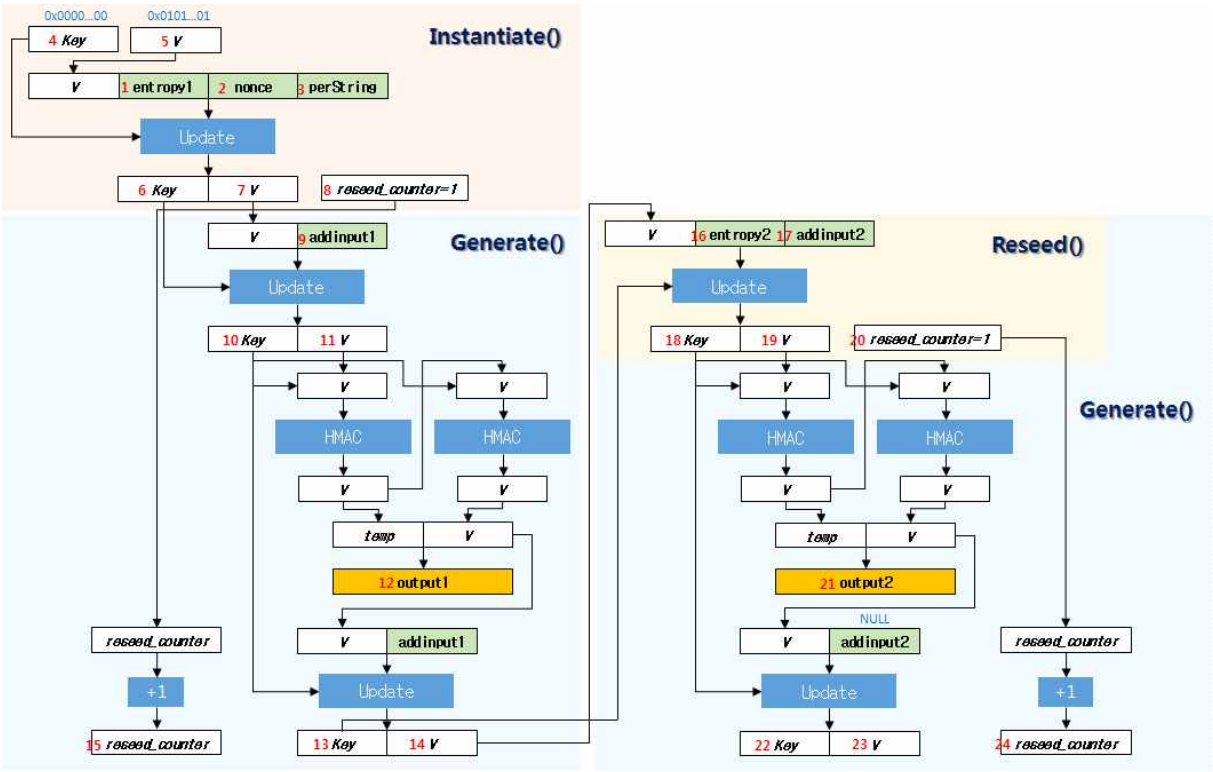
시나리오 1은 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 1로 설정할 경우의 HMAC_DRBG 참조 구현값을 제시한다. (그림 5-1)은 시나리오 1에 따른 HMAC_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



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

5.2 시나리오 1-1 (개별화 문자열 사용, 추가 입력 사용)

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



(그림 5-2) 단계별 참조 구현값 위치

5.2.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	00000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	89E039A0EE9360C6AF38F38CFB065F3712009202501B79AEAAB9FD03
7	V	A6E1E288F188559A060A13A15290818E0C0D1A0475205B0297A87642
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	653DD23F5F1E12CA2CE6033D8541597CA01DB0B102A984A0DAF7E13C

11	V	93406F40D64118AFB579117D1EC067624F09BA8C7DB7DA37C5EA5A66
12	output1	B04C20CFA4535F63A371FFB94D1AD9CF36DEF0FAA96B6ED4A77C48F6690EAB359BBC2E818BA5FBE0BD841032A7766EE67395F584B19A6374
13	Key	A7E8B60712A2F325D241D8CE6CB059F121AEDE221EE1010A7E137384
14	V	F29048ECE17A1C1B2FDBB9F9681B63737C160F27C4B1D30D85B764DA
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
18	Key	09C7B7025438818624FF179A30EE8247912DC5620148507C1E03357D
19	V	5AA5A3B020FD5D221D7B6260451B2A95B43F38D67CF59EA0173C3816
20	reseed_counter	1
21	output2	276286D62CFF5A87C9DF303C7287CB5A5A3D024F9E786ED9273ADD3BDF0BC65633932109C293D5D68531BE8E6D552A76F2D13DF1C815E21C
22	Key	15A9BE0ADC3D3A1A1BE7718C735CFF7CBB6570404057DFDE4F4D4C4A
23	V	8E6AF07B61F39250DE6EEDEE8D77F67E0A51958FC473E62FA785E537
24	reseed_counter	2

5.2.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	70CE78A92D5516CA4A18949AE8647287C53E582D9A5431FBDF2A4B46AEA76ED5
7	V	650B2D9D8EDC29701D07C31C1D68ABDD981B48CE09B29671EA8B56BA1BE9E0D7
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	348D3C9ACB49B3560606390B2F5ADBCF3FE7C553D4A4DB8E5617A63CACCDA118
11	V	F0A485F83FE4931B02AB32C7987EBFEEC55FB0A14FF1F3A8E5EE10048B6D26BB
12	output1	346746FA80397F8D3B2630AB91B9134B9BF5D9FB26D0D7CBB4CB5C67226F87FABD5C36E979A90D75D98F7FE3BCDC67E81FCADF4CB6E57B4F2B547CA617F011E3
13	Key	0F29710ECDDE1A0219DFDA86A92A03E0AADE35D8963AFCC82A04EB494E011EFB
14	V	886542DDE7D2671A3FD1360B0C1694E034696A70D66726C9FA0F61794855F701
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C

17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
18	Key	90808AB52E10A589A9997C6D90D141758136E4CECEF71BC67AB00E6F4DA7213F
19	V	51FDCE7BE2CFE19309CF538C7CDD7908A8D5112C617BF7C59E049FFF1664082D
20	reseed_counter	1
21	output2	16D35A4547DD70BCC7ACE29DC1F88F14EDD369906864398 99D7DAAD4D96AEAF902806E258717996FF1175C8A7936DC9ECDF78212454EB29C2576ED3333CA4469
22	Key	1FAA17EBB6F60A3AAC910BAAEF37C2ACBE08B89BEC151EEB2EB7292DB5260063
23	V	60C20E9B0725625AF6B33E8C2268E8D0CA819A9D55E6BA2A555B8AB8885445B0
24	reseed_counter	2

5.2.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
6	Key	2579204E7B31A3B78C5DDC1EA8BEC0B54645EC2D1EB29DDBBF0D168DA70679A7FDEEDB5A235FC1D98AFDF97D4CE1C5FE
7	V	F1E31425DE12FDC93FD40D022498F5C75BDE188547F15387BF48387D16E2824C5B518B9CD8710E73F434FD9479FFD4E4
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	A910E4456FEE6B95FA41C8230641FE5C1917B62EF24355E21668DF89EE2C20F7B8B9FC5BAB1D9E873C809A5B8AC31C5B
11	V	B6DF6EF4F0A85A4E715724098120F13412B8A4D2CD953918459F23783DD5CDFDEB7E5C72740EC810ECB812D9A2BAFD0E
12	output1	ABC8B1BFC9A0859CAAB84FAD03833870B9A78E18A88116B5F6562C2DCD306E5D4AD30F068FED4C4BD7E689B74115E674EDC1BD02204146B1C5458A393FD8134978368741EFC8D5B6152B560C3C71ABFDC70F0908748AB318F1AB72E814135E48
13	Key	6AC301B98A190AA24463EBB0B64CE7F56298DF58ED7E5D46618A341513339264E5333211F11C904611E811F97915B7FA
14	V	44F8FDD991AF571FA6F6855412464437BF06268240DD7A559E3604E8562B189D367D04444829A5BE1B1DF19A02D6B23A
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331

18	Key	B6748303D227A9AB11B5BEA4B2CCD5A70CCA339FB8CA607BA5A48D182E9603094F53B762C1506E21E044A36D799ABF17
19	V	F7CA07C6FB19B4C1DE39A169B17E55058A64294C17F015E842FD8531E8EBAB4A5B0C88B6C21DA02E515BFB0310244EB1
20	reseed_counter	1
21	output2	9C37ABF3954EF6A400EAA315146B68069298328B7DD1795E653F9D6A3D70B829A9F9B94E4F7407D923CCEF190A347BEB92E800F412A17716AC96424ECCDDDC4064153F94F96C98CFC98AB62A4E24237811BE6DF7263B81BD9AB03DA28F358D35
22	Key	9ECDD852AB73EF5D4F34E5FE5A16E0CD810590ABD238BA3A4F062CCE3C6C6925F5B41B38D2FCC91B9EB0EE2C4C0E18A5
23	V	7FA4F9D5A4E31C93676802F719CB64F3BCD5CB1BED0F3D7DD415DFC138CAAFB214EFDFE5E72B3187BA5B79B05E721EE7
24	reseed_counter	2

5.2.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
6	Key	D6F07DEDB783BED1A63A3B215325247F1CAD87CF4B9A710BBA2786B5A85200888050BB7E3A33CB18265344CAB4E3EDD053CFDC122BC985F23B0E9B45EFE4CB1F
7	V	6F8E96AC60E7989D3A452EB5B3F1BB6576558F1B621BB4D5262DFE100D371B96F7AC4989A9798E61D89EB8A7DBA8667C649677C148EB9F1AB1CDAF546B0ABBF4
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	77DA9B4DA83210C3AB7FED51681DC60D7A07E76026A31E845B0CD374A3BB338997214C43118936D7B3893637075940874509 1DDBCF2849304A966751093BEE06
11	V	CFEFB5EEA5E8340ED993AE14338D81C675914904F3E1BA642B22FF3C0456DF7044D2304198098A14414EDBC919B737AC89E0171967EB9EBF912D98027A88349B
12	output1	52ABF7D99F80137763C86537EF2047D7480F5CD5326D7ABE59BDAAB9304F54E27CBE2FD0BED7EE0C27FA5A5A744FF2C2BD084FDF04344F44EB1538F75851DE6B39CAA11B75576C351EF0AF0B87767527EE2C885725D9461377AC01C7527BFB65E308BED6174C1D24A5C0905ADE55E60E0E1B1D23DD6907B356DE0CD013FB9789
13	Key	CCF7F469AAC63136F21409E88EB848FC0F5722FCAF2F558EA037660AFE987E5B3B3A0935C3DBBACF16EBAFFC3EEC207C7DC7443BF3BC2EFD924C924F66DF374E
14	V	3920BA6553567ABC60EF69A60088B59AF219BD13DE0D27D1F373A82639761C3E55ECC5F2AAAE10EA40AF1D8FA55BCB769E86137FB69CB071F1A2D38E5E45E68B
15	reseed_counter	2
16	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
17	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331

18	Key	2FE8C9ABB90959D4DCFB8226FD4789893373AB9B45CA0864E09046CDA070AAB8 40E275EB90942EA8194BA17BFE8A3884764DE8907847D7B953D8DADD68748889
19	V	554873AABD0211AC79573A0B029E2DAA72DE588C54501936CB57F846755766C1 B973C4EC18B8D98AA25EF40E2FB02AC067567772B2F2A7D1B2AE5EFA7D8E7922
20	reseed_counter	1
21	output2	EF60488A76B1F6758BF3318548B38269073DB1F3F832825774B3745758EA2127 5649ADA60BE2F86416DE31618B57BD0ABCBED5B2486069E453A7FECA362BB5E1 F573EDB277639CE03DBEF8B1CD732CD8BB256CB46C032BE7C2A86C40C6566656 E1BB575E4C4464AD089D4660B505C7EF1F013B29E4B934FE8277C89768B8C0BB
22	Key	4A025FED7BD90283D58CCCAF73C9727F760C0D79DE8E9281550F63AD3B250620 E97E1DC41DA3BE86B974D455244ADC38EB4777628BEFAF3BC03D3D3F9FDF21D6
23	V	E6B0830D49B79FB970322632445E542BA7291972F999F605D3A82F5E807E8C46 109423CBECEF98064E8A38D9CB56D5DD946989077633AA218D0B53BEE36D2331
24	reseed_counter	2

5.3 시나리오 1-2 (개별화 문자열 미사용, 추가 입력 사용)

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

5.3.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	064CF5F672A3435B678604D87608BD6FD5BEF4386B50EC2DEE4BAB2926ED96A7 52DA6EC8905EFABCDF5B1193D1995FB21736E590C994F16E
	output2	0FD60DEADD20F78C46AAECB03547C85D298C242085F28CC18E92617A2179BF87 4F4E9166E7F975FFC3A5E0E1804ACA5CEFC0AFE89810F09D

5.3.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	584ED24F5BBC149F9F0563C19533F64AB25E51B7A9FB2C8024945DBE7FD7E692 C46120DAEDBAED4F5BC383CB0416195024D06AF7674E630505F2C313EB322C9A
	output2	5C0D607C3ED6A6629AC4E7F852D0FFCCBA11AECACDC6AB51E9CB930C65AE2F52 2AF29665C703ECCAE4D824D1C4F8D9E75CCEC1CF22BE4E46234703A5CECA0484

5.3.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	C213F9EE7A7DBF5C75C23E9DD91278F6B379C8B27C96040661E74329CFD9E45A 44E5D80FBE87F78D0CA509F71E8E9EDDB55C7EE8AAAB85EBF1A383B292157D6C D51B58CFF793D300D9575CD8B29B485CF0F7FAFB97F392A64355F7157E4BD666
	output2	1607DCFD9E86B2D82D01631506EBCCB587E5AC358D0AAD951D5E6671F5CBAA32 FD77E778223823CAAE7F636B01671D04E4ABF7FB5D98EB9DD88F236BEE0A7F19 3CA2CF3AF10D1416443786C9B2A66707E1F6DC2E25275C69321B6CEF361B9859

5.3.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	76A32F694A3B41EC0FB11D5297A4897896B7D6F7C5AB27FA6EA8C14397B79A6F F912CDC5A16ABFDD50FD1B408DA0FA58D8C39311A7DEF5725C586076A5029429 6D622F767FAC70A1591A74D1747D51CE2F421D0450590D4FC2F4F3491FC595BC FA672741DCA974B419C8C7C097D793107DFA844FEC40FEB31164408BF3A16F6C
	output2	57BCF2689F6EF879A0C92A8E2D00B5E751C18B253251239B242DDD54F8A6C3A2 33112D17F498F122E6C248F6F88C905FF8261444EAE8CD3B24A9C0F8174C92B3 B75E0F915201994B220473CA5426B06EDA62453C006DCAAA8CADC1FE4CC44CAE D9FF7A3AE9CB5F42283325BEC1981DA3F34AC0FBA39977D68109B53D62F2AF33

5.4 시나리오 1-3 (개별화 문자열 사용, 추가 입력 미사용)

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

5.4.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	5A8E4FC02892DB4B0583E6870F76B957A4C4AE3811E0D48238676928551229A8 03EE7DB1140A07B11D655A020EF1CDA0E7930E26153C71BD
	output2	CCC17FD60FB94DB4BBC3E47412DC8F21149E1334B860F45C44986FD63D706B52 4A9D1D4B219BB9367B1CEF8D1C54E185A70525DB876979F2

5.4.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8E526B7B536B0569024F6F505B6A25EE336B68A5CD11CBA6BAD8FC04BFA2CD23 A610D5ADD071258A8AA9AC32DE28A04BA256E79DF70F1EA83E0989E5B8B0C708
	output2	643F33977875FDAE149C0249E932D3796A653E973485E9F8F6D7B5A2E51D6E6A 134C20C6F5863E3C6B95736DD6B4486E98C48E98A43AD8FE96780F0797DAC06C

5.4.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	31CBCF8F66EBED55C4916F10E7103FB202E0AE269A1ED34857A447F990FFEF0D 7F9AB921A3CBA0C2A959A77EC06F5138A244B64DDCEAB0842A2C3BEFC0ADFC47 3FDC0AD91B3935DB1CFA7E5A9C9FE7B5C410A15B78B85180283AB0F0836B047A
	output2	A4A4594196CA52C2B7AAF6810617FDA7AC63A059D64703257F01CF8E3BC83123 BB963CC88F9C3F0E3549A5F5218A1F85B761399B89DC54E34DF19A4C99860787 E4C7CE8A8AD7E167CFA129F9974410A18CFE3C9906C2E674E3299E077B8FD8F4

5.4.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	9C1B72145F6556363111F779424BE6C4E98DA6F52B10AA249F47C16D3B90842F 83C73E32406D1940667A323B854E22951EBEAEF0CA22B94F3FBCC1A92AE6359F F0EE8903367EB050428C4876ADB5FCDDBC4A527A8A8123685FA66072DAAAD91B FB5FD1029EB540E0323CE24D1CCEA216E76B5173854B6A35DF4EB08CC43485A1
	output2	A0425BC34864BA7D3481B1DAE0655EB242E9526F5BB2152D874537B29E627F30 A717A6BDF5167369F3B392A821EEB50A1315DAD6E98B4B430875FAEB1C2BB5FE 2A78D2ABFD9E635CA23AF98F90B4FE20CE9ADA4A94C9A71305651BC4F7A92B92 FBBCA25B576EBE987ED77FAE74C34128BE0EDB2D344E5E51C716CB72F0076664

5.5 시나리오 1-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

5.5.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	1C2A53CDB3B232268DFA9080A6DAB81923E9374B12A623092B8020D4F45D49ED 3A9DDAFD38C1B91BF0B7D64646DF4D428F83DE4224B6F84E
	output2	3644F0585F4C4D5DD17D3D5642B9D7EA47C823FE811EF4C1AFF7F422195A1CE8 2231359ACE57A6FA7402893ECD6142810176E050AA7BC96B

5.5.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	10E073A0197476C22C5933EF4BBF5C567D6E51B810F4079A9EF4E6D89CEED32D B2E3349F97A83BDC4AEC7CAA35350C27681CF770761704532E3501DE969F7599
	output2	78A6B0A3284B685EA1E69067C19BB5C20635FE259599C6DB6C4FB8AADF4FAB5F C057150C34FFF658BD4840B9AC2DE92FC13C5647DD11A08888C1D3A7D663DDA8

5.5.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	0CFFC7F57B8AB2A29D649565034E8C76CBC7241271DA367D583791CAA97E1CE6 E7025B82AB07C3DA5C75438F38B20FF2F53323EA07172D45D3FDB0F8F09D9B68 2FE0B036C2EE4ED1B8695ED8B9E434F5BE751DCF6E4FAAD44258CF5360DB2BD7
	output2	83DDB9BAC6A660B0C0DC9E85FD13D013CE50A63776FC1E3BEA503D17979F90A2 CDD567A3BC06AA15D726ABE280F5EFC5318B84031945FFB72063A129BBF63C41 BC780EC47B39D2C2D5ABAE22428FC11DC21BD0114C243761608C27D1FAF79DAE

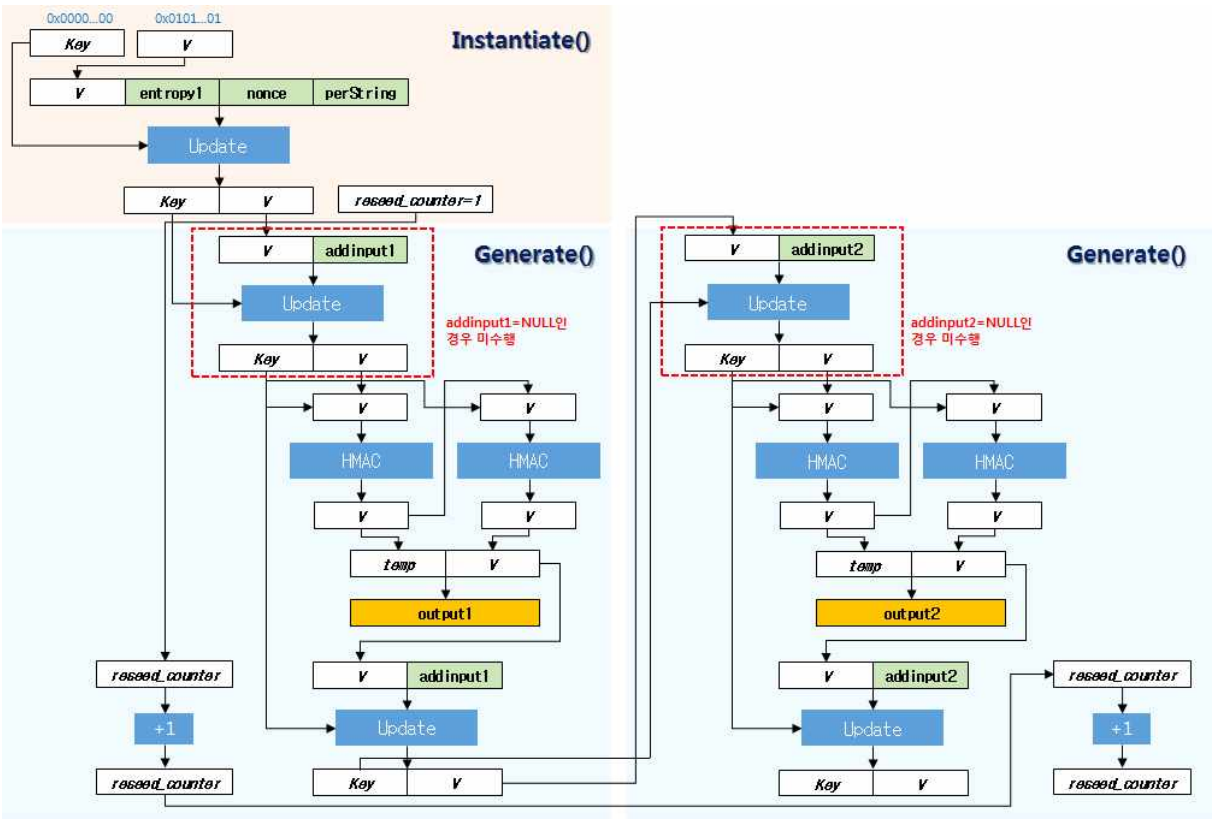
5.5.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	697C261B1558B2C68CB124341557998DB9B8E73877E39468487B32CAD1A25962 54AC99028D9B0D79C6DA9A5A90D7213448DBC10FC2FF9D0F6CEF6A7BB37E1518 F19C5E97914D04D3E7F16D88640016C057DC8E7563D5887CBB51CA3357363788 44EC923FE3C7FC09AED34B7EEB95E4E48682510708B6CF8577D55EF5AAC40242
	output2	41BDE9C388E9A9D2A51F9F2DD38F4A5C4028ADAFBBC70D44BE0BB705547D75DB 76A8453F6A4F767C851F2445931584469B0E37E73A88E595071D46DF90B5D12F 2389EE316E4022276044F8BA9E5468BAE77C25D88E46533D9ACC3AD6A5AFB7B1 3B04CF483DE086C8965D2E420E7CB2A1588A6C264ABAF4D990CE721D17C0D7E8

6 시나리오 2 (예측내성을 지원하지 않고 갱신주기를 2로 설정)

6.1 개요

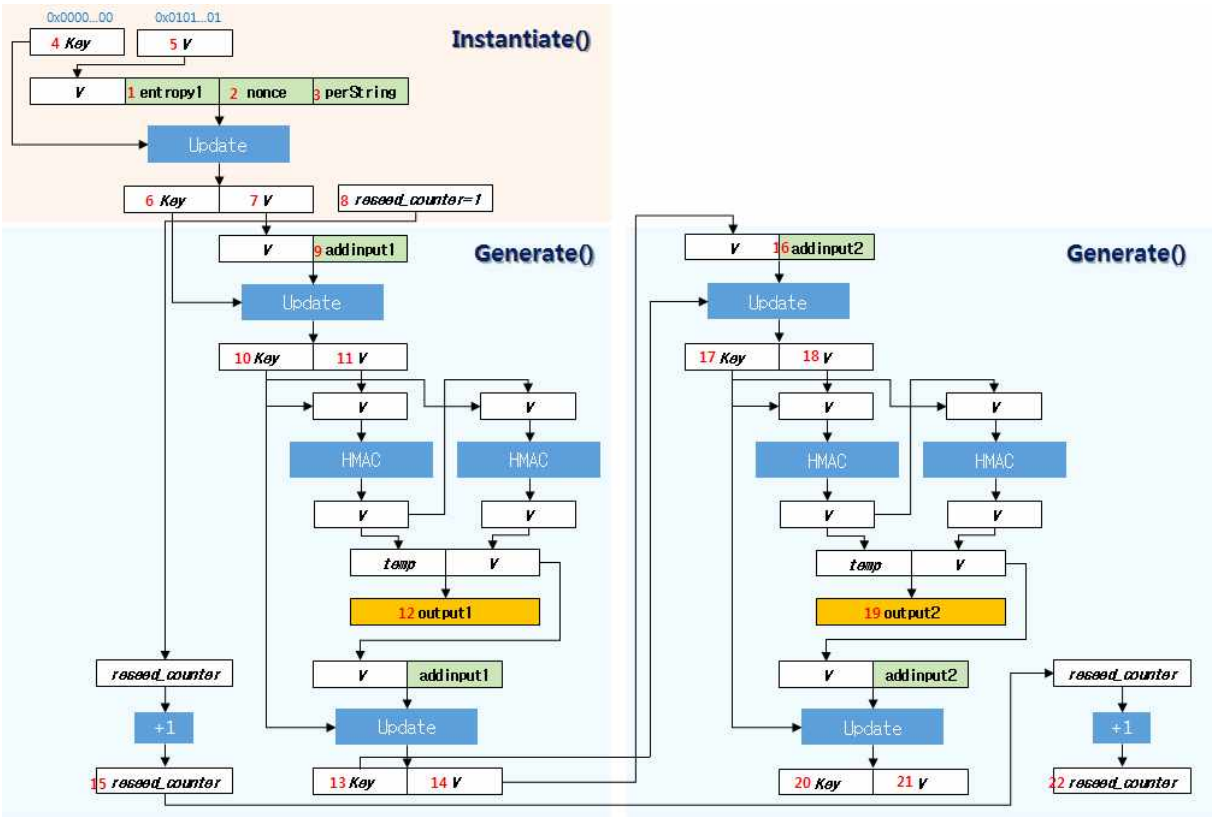
시나리오 2는 예측내성을 지원하지 않으면서 상태갱신 주기(reseed_interval)를 2로 설정할 경우의 HMAC_DRBG 참조 구현값을 제시한다. (그림 6-1)은 시나리오 2에 따른 HMAC_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



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

6.2 시나리오 2-1 (개별화 문자열 사용, 추가 입력 사용)

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



(그림 6-2) 단계별 참조 구현값 위치

6.2.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	89E039A0EE9360C6AF38F38CFB065F3712009202501B79AEAAB9FD03
7	V	A6E1E288F188559A060A13A15290818E0C0D1A0475205B0297A87642
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951

10	Key	653DD23F5F1E12CA2CE6033D8541597CA01DB0B102A984A0DAF7E13C
11	V	93406F40D64118AFB579117D1EC067624F09BA8C7DB7DA37C5EA5A66
12	output1	B04C20CFA4535F63A371FFB94D1AD9CF36DEF0FAA96B6ED4A77C48F6690EAB359BBC2E818BA5FBE0BD841032A7766EE67395F584B19A6374
13	Key	A7E8B60712A2F325D241D8CE6CB059F121AEDE221EE1010A7E137384
14	V	F29048ECE17A1C1B2FDBB9F9681B63737C160F27C4B1D30D85B764DA
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	FACFF0F4B2975C69FD2D17A82004FCEBDD8BEE7B8CEE804B56DF6C2E
18	V	5B0F9E007EF9256F7EA26E92EF8352F459115A05B847A073BCC6EB7F
19	output2	F75BB5D2EAB6FE9F1BF0657FDFF280A30B23C5ED910E6DB49B2D72C42A2A96C571F31D9B8334EFE0619FD6B07EE08B84A92CACF922900FD0
20	Key	9668F28CC7D7C2CC84E63DDE59544F274A73DF19BB5536790874D069
21	V	1FE2E60870E4B16A34E9B5CBF2326DF67CA297DD686875355559ECF7D
22	reseed_counter	3

6.2.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	70CE78A92D5516CA4A18949AE8647287C53E582D9A5431FBDF2A4B46AEA76ED5
7	V	650B2D9D8EDC29701D07C31C1D68ABDD981B48CE09B29671EA8B56BA1BE9E0D7
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	348D3C9ACB49B3560606390B2F5ADBCF3FE7C553D4A4DB8E5617A63CACCDA118
11	V	F0A485F83FE4931B02AB32C7987EBFEEC55FB0A14FF1F3A8E5EE10048B6D26BB
12	output1	346746FA80397F8D3B2630AB91B9134B9BF5D9FB26D0D7CBB4CB5C67226F87FABD5C36E979A90D75D98F7FE3BCDC67E81FCADF4CB6E57B4F2B547CA617F011E3
13	Key	0F29710ECDDE1A0219DFDA86A92A03E0AADE35D8963AFCC82A04EB494E011EFB

14	V	886542DDE7D2671A3FD1360B0C1694E034696A70D66726C9FA0F61794855F701
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	B462471F3C905F55845ADDC65DB001D0E7A766039E82C8F25394A7972C9C327C
18	V	50B6BB3BACD33BFFFDA699CE7F304D005CF366F58634EFBDCA255FD3237DFDCE
19	output2	36708B910CD4F1115F6BC27EE23CBE21476092F90064A4E0D8DD302E6CDCDFDD9C7D4E0804C851218ACFC5369A8246C8536731A19DD347785348C1E8F2550991
20	Key	8DBE30E9102E8946D57209AFD8111D45BDB2B5453F7F782BEEF395AE7AF34A9A
21	V	8D456BF9AE6A43D53760856ED8CD043B22160E7EDEBF00E95FDC7D1E53F4F409
22	reseed_counter	3

6.2.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
6	Key	2579204E7B31A3B78C5DDC1EA8BEC0B54645EC2D1EB29DDBBF0D168DA70679A7FDEEDB5A235FC1D98AFDF97D4CE1C5FE
7	V	F1E31425DE12FDC93FD40D022498F5C75BDE188547F15387BF48387D16E2824C5B518B9CD8710E73F434FD9479FFD4E4
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	A910E4456FEE6B95FA41C8230641FE5C1917B62EF24355E21668DF89EE2C20F7B8B9FC5BAB1D9E873C809A5B8AC31C5B
11	V	B6DF6EF4F0A85A4E715724098120F13412B8A4D2CD953918459F23783DD5CDFDEB7E5C72740EC810ECB812D9A2BAFD0E
12	output1	ABC8B1BFC9A0859CAAB84FAD03833870B9A78E18A88116B5F6562C2DCD306E5D4AD30F068FED4C4BD7E689B74115E674EDC1BD02204146B1C5458A393FD817497368741EFC8D5B6152B560C3C71ABFDC70F0908748AB318F1AB72E814135E48
13	Key	6AC301B98A190AA24463EBB0B64CE7F56298DF58ED7E5D46618A341513339264

		E5333211F11C904611E811F97915B7FA
14	V	44F8FDD991AF571FA6F6855412464437BF06268240DD7A559E3604E8562B189D367D04444829A5BE1B1DF19A02D6B23A
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	48F4EEBBBFD5DF780BB1FC46333B8C538C406F808BF6404D97D3463EFE5CA819201050BE78DBC4A59E5B85FA61C98C1F
18	V	7EBE77BA8B58AED1C825C16F649335E5869F75F8BA48CD40955622413F5F0BE0CDFB813F789B06CF3F30BDC30D2ED6E5
19	output2	80F4D66EE5F03BC29D1506FF42325E9D238B489473926E388D32F79D29BC49DE3EEB9E8616DCE4AF7896D8F70ECE9195E8884B320816FA70D0387AF0301005C81D58292541A74AC6CCE9621DF8633F917D9A71CE587E4284CB6AC49187292F45
20	Key	B1E799895A64EF2B72DE20D8FFBDC9BEBA14D2284AE19D252A93A7BF2E8ADF7264ABBDE8A8DC261214A74F38ED0D07D6
21	V	ABA5C70FAF6B9F9C84FD682F467ECECE959ABA70B94F23209B8FF848E2502B5BACCCE81BF2B979B4CB99301D75E69657
22	reseed_counter	3

6.2.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
6	Key	D6F07DEDB783BED1A63A3B215325247F1CAD87CF4B9A710BBA2786B5A85200888050BB7E3A33CB18265344CAB4E3EDD053CFDC122BC985F23B0E9B45EFE4CB1F
7	V	6F8E96AC60E7989D3A452EB5B3F1BB6576558F1B621BB4D5262DFE100D371B96F7AC4989A9798E61D89EB8A7DBA8667C649677C148EB9F1AB1CDAF546B0ABBF4
8	reseed_counter	1
9	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
10	Key	77DA9B4DA83210C3AB7FED51681DC60D7A07E76026A31E845B0CD374A3BB3389

		97214C43118936D7B3893637075940874509 1DDBCF2849304A966751093BEE06
11	V	CFEFB5EEA5E8340ED993AE14338D81C675914904F3E1BA642B22FF3C0456DF70 44D2304198098A14414EDBC919B737AC89E0171967EB9EBF912D98027A88349B
12	output1	52ABF7D99F80137763C86537EF2047D7480F5CD5326D7ABE59BDAAB9304F54E2 7CBE2FD0BED7EE0C27FA5A5A744FF2C2BD084FDF04344F44EB1538F75851DE6B 39CAA11B75576C351EF0AF0B87767527EE2C885725D9461377AC01C7527BFB65 E308BED6174C1D24A5C0905ADE55E60E0E1B1D23DD6907B356DE0CD013FB9789
13	Key	CCF7F469AAC63136F21409E88EB848FC0F5722FCAF2F558EA037660AFE987E5B 3B3A0935C3DBBACF16EBAFFC3EEC207C7DC7443BF3BC2EFD924C924F66DF374E
14	V	3920BA6553567ABC60EF69A60088B59AF219BD13DE0D27D1F373A82639761C3E 55ECC5F2AAAE10EA40AF1D8FA55BCB769E86137FB69CB071F1A2D38E5E45E68B
15	reseed_counter	2
16	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
17	Key	4F54A4815895033BE6611A2C89FAD69414632BF63A8F6398388A28884B8B4F6B 1CBCE8397F3F44D51AAA108190927ED9C87129127F7EE238EF040538C8C5C9F7
18	V	8D8CD904E18E7D66688CF18578B33480C67DA154B2631B968471B7456D43C0F7 BA930F939A9541DEE2B606B7A7F47D51346CE548371A68291A55ED47E94D4CE3
19	output2	06BB04BC6FD1AEDD4C35DE6EDA5F466AF5D2B2A939C904100F05600138187C95 2044EDEC6962B844E872583473E9CBCD2D63346FAC0D8AEB8DE5469E5FADFACD D4E4B1C157F0CAE80E7646657ADE22FAA96745E0ACD271C5A3112E021D38D037 8A1938085686577D422A9CFAD85414667F2F096840C22FFAAAA4B0E4C5A4B8B9
20	Key	AF69147262FE3B47824BD1A8B4FED0C97B03867F044C863EB876038F34F5B589 ACDE700C5D42DA4868F3F9494F939FC7925BD455D160B2B4C34A939210DFDB6A
21	V	2F272CD5EB3CA0D2B67C1F259885B6D3AD00D1F666CEA0D292128A0CE1AB69DA 905F86DD39B2141739FF98D5A057A270D5BAB4F88EA8D8557A2F18E29E4FA429
22	reseed_counter	3

6.3 시나리오 2-2 (개별화 문자열 미사용, 추가 입력 사용)

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

6.3.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	064CF5F672A3435B678604D87608BD6FD5BEF4386B50EC2DEE4BAB2926ED96A7 52DA6EC8905EFABCDF5B1193D1995FB21736E590C994F16E
	output2	B234F932B2A3D223C3AFB94FDD6F3781D77379CD6032F5CBF2279BBB22484424 7CD0C0DF69272C9A21484BA2F9CAF0DB95068C03553A2B5F

6.3.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	584ED24F5BBC149F9F0563C19533F64AB25E51B7A9FB2C8024945DBE7FD7E692 C46120DAEDBAED4F5BC383CB0416195024D06AF7674E630505F2C313EB322C9A
	output2	A423C9DCF931595DB5A00E99ABD3160AD6BD1DF327D98F0F151AA426285C9AB6 000DD88BEA2989D150764671CEAB9105BC2039EAFD6F1E6494BDAEFA75C56A45

6.3.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	C213F9EE7A7DBF5C75C23E9DD91278F6B379C8B27C96040661E74329CFD9E45A 44E5D80FBE87F78D0CA509F71E8E9EDDB55C7EE8AAAB85EBF1A383B292157D6C D51B58CFF793D300D9575CD8B29B485CF0F7FAFB97F392A64355F7157E4BD666
	output2	23B5BE14AEF658AA192580DAA44201E7556CAF14C7D123FEBC243C4BD5BAB929 0DD3DFB00A7C95C1175AAD9E577E71D9F0EDDAF28A436F5BE12F4EF13BD2D33F 341A9D714741ADA44A7997F55007B6A8DEB0DDAA37C7CDD12A78CB406AF4C40C

6.3.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	76A32F694A3B41EC0FB11D5297A4897896B7D6F7C5AB27FA6EA8C14397B79A6F F912CDC5A16ABFDD50FD1B408DA0FA58D8C39311A7DEF5725C586076A5029429 6D622F767FAC70A1591A74D1747D51CE2F421D0450590D4FC2F4F3491FC595BC FA672741DCA974B419C8C7C097D793107DFA844FEC40FEB31164408BF3A16F6C
	output2	C82408B4C0DB63977833D521D37C1296E57484BB87FE9C67AD9099644C02794E 38123EE36F4DEC1CAEED77D8A13FD67BF72B34BAC6B57502E2CA4076BE980566 7299196569945CF05B4D3386E20391B5FA08AAFA6CD151BF1E526A8722858D0 00D0ECF689A16683D78948E0D71BB7391CA57417CED82EF7D977EA3590BC6800

6.4 시나리오 2-3 (개별화 문자열 사용, 추가 입력 미사용)

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

6.4.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	5A8E4FC02892DB4B0583E6870F76B957A4C4AE3811E0D48238676928551229A803EE7DB1140A07B11D655A020EF1CDA0E7930E26153C71BD
	output2	FE6C24B57B09367B4911A65B9CE21081F9595B2F7C56673F6664AA563374FCCDD3F2D5F90980D088C6B0ED7466EE6145FF65E9A07E501CE1

6.4.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8E526B7B536B0569024F6F505B6A25EE336B68A5CD11CBA6BAD8FC04BFA2CD23A610D5ADD071258A8AA9AC32DE28A04BA256E79DF70F1EA83E0989E5B8B0C708
	output2	4C95C7C169762F384B70433A2E4C561D2847165107F3268946B8314EE9F6C72F326D32A768F77B48EFD4B7F405B760CDD8F9B24E5C92E310DD53B895CFB7893A

6.4.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	31CBCF8F66EBED55C4916F10E7103FB202E0AE269A1ED34857A447F990FFEF0D7F9AB921A3CBA0C2A959A77EC06F5138A244B64DDCEAB0842A2C3BEFC0ADFC473FDC0AD91B3935DB1CFA7E5A9C9FE7B5C410A15B78B85180283AB0F0836B047A
	output2	3F658262183EAE5A89FA5A1730267268D104C18DF62FC33B0903B3768633C29283B4EFD006DC07D7B04C761998443F1D66B817B62B810F143C647A51DB5618033E357A7F23F51A8307B1884CA89DCB739781DB2E31FBF80AE0E1C8B3AA8A1C8A

6.4.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	9C1B72145F6556363111F779424BE6C4E98DA6F52B10AA249F47C16D3B90842F83C73E32406D1940667A323B854E22951EBEAEF0CA22B94F3FBCC1A92AE6359FF0EE8903367EB050428C4876ADB5FCDDBC4A527A8A8123685FA66072DAAAD91BFB5FD1029EB540E0323CE24D1CCEA216E76B5173854B6A35DF4EB08CC43485A1
	output2	BB5E2EA5214169BCC0C1935B13CA1442501F6795B172D5059B29A3B0CC64A597B063B6CE9C6A2BCFF3806D6B26C3A8A8FB443BCC391B09D63117FE03218DCDA14037E4E47E133A937B2067E14104A71842EE7C612F6B1FEAEA8A9596B751DDBD02B5A4CC4B21AEB6479F39A612FD8025FD47745976D9F4D51C5EBFC34C47F011

6.5 시나리오 2-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

6.5.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	1C2A53CDB3B232268DFA9080A6DAB81923E9374B12A623092B8020D4F45D49ED 3A9DDAFD38C1B91BF0B7D64646DF4D428F83DE4224B6F84E
	output2	CB725B48FFF0E0CC0E704BBC78A27609889FBC8F23BE8BDC1C834E639A9C88C3 3B573DF29F5C7B9C675CD08072AEBA57C1C2C78277E09681

6.5.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	10E073A0197476C22C5933EF4BBF5C567D6E51B810F4079A9EF4E6D89CEED32D B2E3349F97A83BDC4AEC7CAA35350C27681CF770761704532E3501DE969F7599
	output2	77EF00FDBAEC13D66BE95956116ECB86105EF339B7D1ADA888076E67DBD44FA0 FC122874BA193A001D3234F8E510B2A44A5677BE646EDCFF017FA15E3E756C19

6.5.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	0CFFC7F57B8AB2A29D649565034E8C76CBC7241271DA367D583791CAA97E1CE6 E7025B82AB07C3DA5C75438F38B20FF2F53323EA07172D45D3FDB0F8F09D9B68 2FE0B036C2EE4ED1B8695ED8B9E434F5BE751DCF6E4FAAD44258CF5360DB2BD7
	output2	91676725A3E8C6533A507122AC08B866102D1FD74F77132B452AC6ABCEC4DEAE 1C97F2FE95BDB904F25BA9EBA3A65A3824E1F669CE0D4DBF1C78EA3D01694923 8A27346B16F3AD65AF950ACB35276D7963DDAE67F8E16B5244B0F91634D6514C

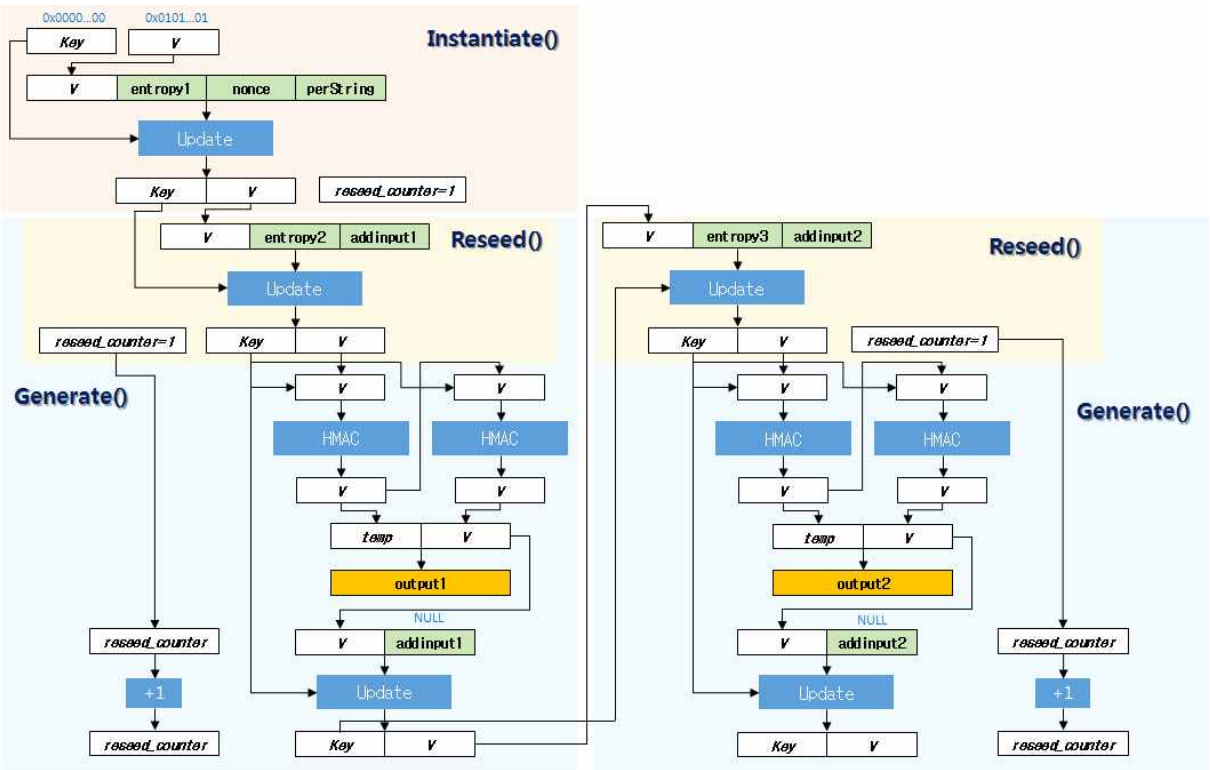
6.5.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	697C261B1558B2C68CB124341557998DB9B8E73877E39468487B32CAD1A25962 54AC99028D9B0D79C6DA9A5A90D7213448DBC10FC2FF9D0F6CEF6A7BB37E1518 F19C5E97914D04D3E7F16D88640016C057DC8E7563D5887CBB51CA3357363788 44EC923FE3C7FC09AED34B7EEB95E4E48682510708B6CF8577D55EF5AAC40242
	output2	B0A472D0ECB120D63EE322DE6AC9FAE51534427A2CC6A4D2C72C6CD514463E08 3E3322CC124A91D7944433110016 4C05802DB88BA7ADCA65CFCE163FBDE25E27 70B335C957EEDF14AE705AB9B807586C2505F309E253F0A3BC7798FB728B2E95 43EE71F1DA64043CA778C5BF5B185BAA79B09B88904AF5E17C7FA9C9E3FBDC06

7 시나리오 3 (예측내성 항상 지원)

7.1 개요

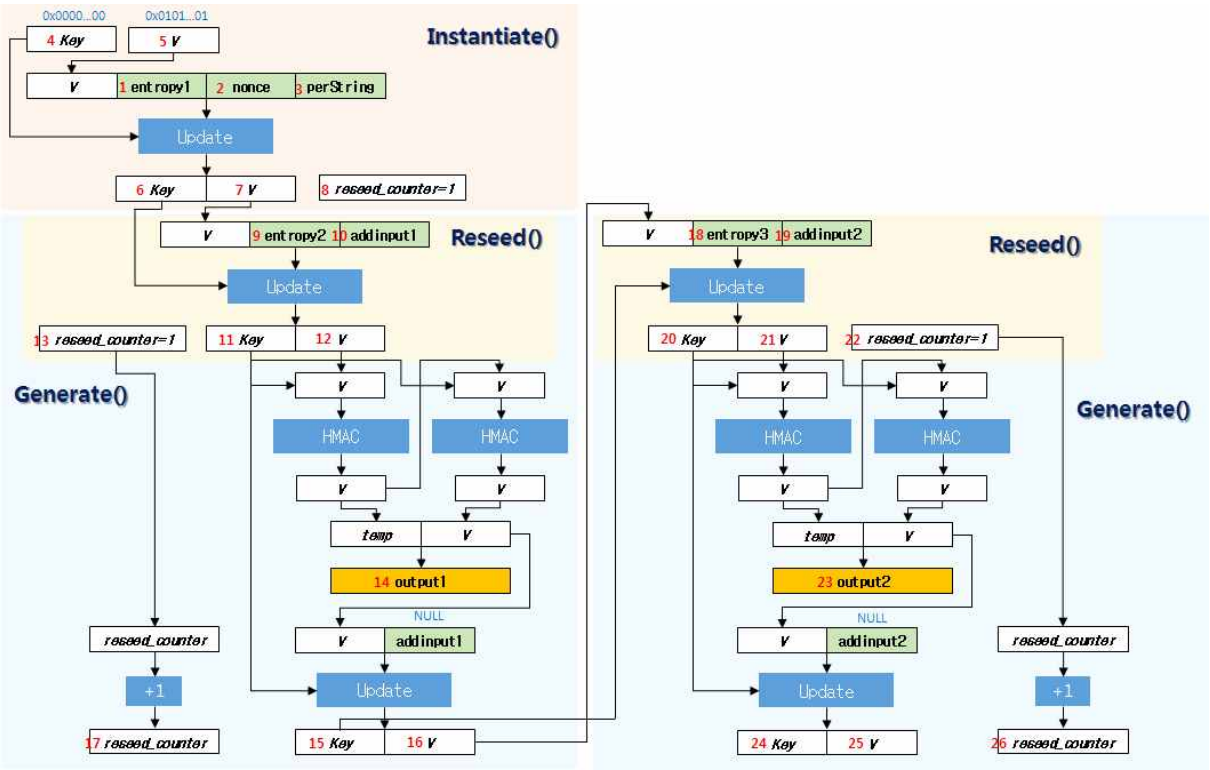
시나리오 3은 예측내성을 항상 지원하는 경우의 HMAC_DRBG 참조 구현값을 제시한다. (그림 7-1)은 시나리오 3에 따른 HMAC_DRBG의 동작 방식을 도시한 것이다. 특히 개인화 문자열과 추가 입력의 사용 여부에 따라 시나리오를 세분화하여 개별적인 참조 구현값을 정리한다.



(그림 7-1) 예측내성을 지원하는 HMAC_DRBG 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 HMAC_DRBG 참조 구현값을 제시한다.



(그림 7-2) 단계별 참조 구현값 위치

7.2.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	89E039A0EE9360C6AF38F38CFB065F3712009202501B79AEAAB9FD03
7	V	A6E1E288F188559A060A13A15290818E0C0D1A0475205B0297A87642
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C

10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	AFA0446C83D76A200EFD18C9B046530D3BB0B884232121BFEE6C84CC
12	V	0284167C9E652CC893616265A2C37575B3D6C2911BBCD52D77F02557
13	reseed_counter	1
14	output1	D4499871E95EBF021F882F8A53F7B610F01A2A25456BD24DB87C9DB2E01A75CE FD786391213CF9621962542DF5B7AFC8C234383CE2A177B5
15	Key	8D8C5089AFAD92BECAE0790F086651E3A7448E7D5BBB0D0D0645D4B2
16	V	0366B578A4ECE130A770D447FF3C9A838C90106C82B1B4CE9941264D
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	2B9A44721D726AFD9BEF7888F7FFEDD5EA2461B7C8FCAC008E641080
21	V	595D62B48498F1EC34988E3796F296DBE021D43EB5656EBD71B55F6F
22	reseed_counter	1
23	output2	837495B21B9C2A254E08966AD4A5A61591529F635FEB05F63F4B6A1F9E2FE8DE D3294B73A517E00F5C5CD360B4D8A19E0805F739ED9E786E
24	Key	30C0CA39EC1C6B8571AC324894303BFEAF1C1ADFD1668E44AB16C0F7
25	V	18005EE32BAF98537E94CC87F3F3AC191FA1D90371DE13B275492B67
26	reseed_counter	2

7.2.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101
6	Key	70CE78A92D5516CA4A18949AE8647287C53E582D9A5431FBDF2A4B46AEA76ED5
7	V	650B2D9D8EDC29701D07C31C1D68ABDD981B48CE09B29671EA8B56BA1BE9E0D7
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC496865150007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951

11	Key	C992A11C1F164BACC4FB5DDEFCA2B1C4D698446907CDF21712DD80D7403A30D9
12	V	71B0055571701ADFF15C5A193E3C7DBC275F0FDD2117FB55733BCE0AAF09248E
13	reseed_counter	1
14	output1	B27CD15CD68B5E118F01A8A848A2E647B34CB45E80FC53FF6FE26A56472E8171 B9186DF4DE9763395A1CCBA3C677DB3DB020376C01873B18CB8AD4EA5844CF26
15	Key	F14105F1C82DDDDCE0FEE73EDD6A3DACF1E90421763DC2D08C46964CE54D2843
16	V	E3EB7E00E64F926469CAFC89A867A2D6E48631DA2C2040FC16748792EBC24EDF
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	4CB8BCAEE0B7E66320F37E6056195B24776A031AD97EAC880FA3C5DCDA5D1B93
21	V	0B277064C83E87FA61F601F9993626A1E02D0C564A38407C9DABA72E894C8960
22	reseed_counter	1
23	output2	ED5466F9569EC0EA7F63A120E322967A9734829D5E3181DE6DEC0F3A0FFCDBE3 0141A9C9129C03213AF3804FFADB8786125CD1E35DB05A5FAFD1581824875D8D
24	Key	16A1FEF00AEAA2E38BD007CD53F46F4B47EA88CC1D53C35182EAC21EB3C6E25E
25	V	9DB8E29BDC45435ACBB8AE0A1E0F46C6BD9FDDD185FA64E68970F36D5A674ACA
26	reseed_counter	2

7.2.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21
2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5	V	010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
6	Key	2579204E7B31A3B78C5DDC1EA8BEC0B54645EC2D1EB29DDBBF0D168DA70679A7 FDEEDB5A235FC1D98AFDF97D4CE1C5FE
7	V	F1E31425DE12FDC93FD40D022498F5C75BDE188547F15387BF48387D16E2824C 5B518B9CD8710E73F434FD9479FFD4E4
8	reseed_counter	1

9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	653E00441B246A9546B7AF6D8B5D8300D26521FA3FE0A1484C102710C3A8B953 6D6301DE1AFA91EC822B1321BCBB2E44
12	V	70ADE8D623DD5013B8969876F3156F64661DA6E8E1B3A60CB0C8CA360D5180EB 271BA4632E7B5C4E92C43AD23AC479FE
13	reseed_counter	1
14	output1	C37631495316581EDD1DA54BD0FAEB0592C9100F2C639B810695149D8CCEEECC C22EA2DC52C81469415363A618088E97B669063A0F32BE4ABB35FA07029EE8D1 DF2BDDF874CE00ED9C7BE2882B29754E75EC9BA7F220D0CB689067F443E78FC9
15	Key	A62170BA54328C0411B6ABCF2032E1C6284DEDDDFBB2BEE100E84C3655D93E84 E8528676BD0795CC75871936EFE3B800
16	V	97C94BB412DDE8C0841252FA6FBC2566CC6EAF0925BA7606CD31E941653FC78E 8CDE32B4D235CDE8908D51D6D3E4CC2F
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	DE49542B097796D30785DB2FFF63780CE3EFE2CA6B8624633F7555101879AAF3 402ED979685D794EE911629BA656B334
21	V	A7EF1B151A6EB5C6B5AF04C4931561184DD844A7732317D06946D0F7B40B1D3F 3E6245BB683E7BDEE4D1BB50D5E3EEC1
22	reseed_counter	1
23	output2	C5222F4941AAC236465AACA542D60A1FECA0466C25C9B784EEC31926CC1966BD 36BBA53885A83E8C87D26E00EE78B023891E96BC4B57D6652A5D082D8AA6DD69 E0CC491A7868A02A7CD8215BB17FF0C462BB1AC725F26D7F94119CB51FF56552
24	Key	EC32BFDDDD103854C7E8581398125F6741D5EB3442D2F16935B89D709D3D99B2 9B491A04EC0E8857725D29FB5158A5FD
25	V	2884203CE311BBDC0E28D5657F8B8B3247A47C2C5F51B391B3CE5DEE3BD4877F 379999D02EAE137F2A4D01AEED3A9FC2
26	reseed_counter	2

7.2.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

위치	변수	중간값(16진수)
1	entropy1	7145910782ACCB48308ABB1C0A4107227B9F1AA8F26A6CD53F3C032741913A21

2	nonce	BE1FC13D9266E5280C87112E955995F3
3	perString	A1F6BEBDAF3ECD15519841753BF5147DE010E9D693FD4C68EC053ACD6EB1E405
4	Key	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
5	V	0101010101010101010101010101010101010101010101010101010101010101 0101010101010101010101010101010101010101010101010101010101010101
6	Key	D6F07DEDB783BED1A63A3B215325247F1CAD87CF4B9A710BBA2786B5A8520088 8050BB7E3A33CB18265344CAB4E3EDD053CFDC122BC985F23B0E9B45EFE4CB1F
7	V	6F8E96AC60E7989D3A452EB5B3F1BB6576558F1B621BB4D5262DFE100D371B96 F7AC4989A9798E61D89EB8A7DBA8667C649677C148EB9F1AB1CDAF546B0ABBF4
8	reseed_counter	1
9	entropy2	92BAA7658C23A7EE8E80A8EECF3E2B6891A52DFC49686515007AC763F9244C8C
10	addinput1	6625B06B16AF81E713A03866EC5B7B870CABB597E25A5DC03FFF7C7DFF176951
11	Key	8ECB2C4A31E6EC3D1914EED2EB55E29326C5C8101A586F353C427788BECF55F6 D9BA9039FABCC2EB533E45C013A343746922306C627691868F223B5F0E528C7DB
12	V	8FBD15F526D1386E73DC8A066359FB82BBE0F7BAF2403DA56C1E92E641D45775 5CB5ADA742B5BC022510C969C88529CACF007A22E91BBB629E7BA8B548298438
13	reseed_counter	1
14	output1	15202ABE016547BA319AD38174E635A9DB6F18571FE1603270E98B2D2C242B95 051D5A1E19E3FA98208E251A49B425795370EFB5C5A5DA718A0CD838D1A82CF8 1B2A7003DFD02D04174A1AB2473216DFE9637C7363821EFA970F920DEEAA1236 2740BB391EBE1A4B1F992DEBC311F6DCB3AF044D57AA28FBC5C13C924A627253
15	Key	31362D946AEE1DE9C9498A64BA16F2292276F5F3281856F49D590AD5228D4E8D 64292A44A92F34EB1106EECF8D887214DABDCC599EA4B5362C993E3069151C91
16	V	8F9100AC2986261063F2C034435ADA7B1DBEDBF3EDBD88254F060BF700070703 8C463587994793E25C3B4BA27D57F6AD0257B0AD9096F9A0BA9657C393390 9C6
17	reseed_counter	2
18	entropy3	F148FD648C2B7BB09395FF218C07D367B8CCE93A3B881F937E14C11DD2894FE6
19	addinput2	EB57D7B9DE41125F27F686902F4B81F05C1E3A6D34EB1171C69A185C459BD331
20	Key	E636BCF4D28DC0BF0FB16BAAADB64519C42468C648BC2A75BAE97BDACFEB80BD 316A1580616B4DD6C741AC117862A2CCA3C916FCEC52471B0A70F3C05113AEFE
21	V	6191E254D54152BD5A2FB812B813209E48C3AEE989543331 2B6A47D2C0DF5F9A A9091FF5B095185E366CF350C7BF72908ECCF92A0D60F5B8FAAA6B96B0633E13
22	reseed_counter	1
23	output2	FC0C72E5B82129D10AF7A5B75395A4FB0090ECFBEE59B0C69EA63F97DFB87059

		E9CBBD92349EE25DACFD825E948F97095E397EC213B85515460B3903A277D9FD 4BB5597B449925EB4CC1B067EF8EABC988B1785B6C83297E35D32325A7559AB3 021212C656E865C1DEE34709166F0FA4D4FC616B34B0E5FE1A7AB366E155ADC0
24	Key	9F22A03FA202F0C9BABB3121172C5D950B6C5128A2610552E240B4E928C17003 5C975657FAA95A23D43787EAAEA563309B8C803D43F10642B3B4A340BBCDAAC5
25	V	4CFBAA33F965256C95C7F0679430926D44BE11A3AC732224A3C07294A3D0C34D 9A3A2AADC4E117D761237A81C2D4041DFC8C109D82DBC1F506E7EB4883586CC5
26	reseed_counter	2

7.3 시나리오 3-2 (개별화 문자열 미사용, 추가 입력 사용)

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

7.3.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	5DCA1345676D28F430AAFDE9D91D503C328C8D0159C5A95427DFB4D1DA36D22E 6ECF5A91BDBD27B6DC08208EE4179273EE0C37A25EF7CEA4
	output2	27E867654A9EAEE21DF2A5CD2616A9919E7B500D02712901ECA540854FADB911 AD5D6F306AFE1C73075B21DD9081F20F625023D140C57770

7.3.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	A9148B16CA2CE01C7BAD7C12A262CE74CC37323693A5D6F4B81A52E9F14DD733 0AAAF0BDF364A1BB98CE97BFC349869B96CFC902CB6AD852E46A482454E60245
	output2	4F4691EA8F353FAB2E607EDACEE79266662 1A833F912240E9E8BB2945B04D4BB C2E29A516A693095DB5ACEBC5EA0F5E3108DB10BCFA415E1D6A88DDE78DC8530

7.3.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	CF4E514EDB922495A74880E230EB2A16724138D8394A7B6674D4F0C8A79B6B46 BB373136DCE6D51E5544E352574DA434D570C0453BFFD845F4A8EE2E649DCABA 1A278972384717DB25E553CBD2DFFFC9F3AC380A84F0A13F0AF5828437F03142
	output2	D13D88F82B5A1A35C3C4FFB5A3688929BBE308AB3578BE732765D378FBD36D43 E87707EDE0CC76C1E115B27BB562E15F99B371BFA049FBB03C9B97671E14EF9C 46C7558B9759F707AA53A6009D5B23BA94AA712A67505D926C798924B2D5E8D2

7.3.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	17177931616195FB5582C9EA4900451C41BBF9A7F55AE8E11E913ACCDBE0EEDE F3FEBEE654B628249409EA57E3F86249153D339194190F4B289521FD5415AC51 9AA55E1CA1059A311BDA76B039BD8AD97F29F48189DEC37C579D6E874DF2825D 06CEB842731E06924348459CAF1E7EA333D38919D74846EF6E739678AE561BE0
	output2	0031771873FCEDABECBDDF74A673F29E753468648DF10564457E09A9117CDB7F CD78030C8B3E0070A4FAE05AA0EC1B7D5A49454494C76082D98514CA8C6C7E65 288C5385831B9297B0A474D9314F69DA3EB894E566AF23944F0E212DE74ED1F6 BD3F591FA6CA05866CC60BE2E650F4752CF12C69430CE85F1B04D18EDC0A840A

7.4 시나리오 3-3 (개별화 문자열 사용, 추가 입력 미사용)

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

7.4.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	722F9CD4D8B70490B5F71D3FA8C9DB903AB057F8AC118A5331907BA9AAB66FBB 3782B64274D7B775B154F11508FCA38145CC6461118 10ED0
	output2	13FF8D2B97BCC436E91CE4B807F0F8234C309FFF4DD743F7B27C1DBA3C5E46A0 175E53160F9C2C421AC7DF35FCA843E4F66026AA266E53CF

7.4.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	B0564F6157526346F44CB26024F4B8544C98F9110EBD2A9A56952DEF923AE75B 5F07CDC3905143E8F0FF96C477430CB5AE1B35A08105B32B7AD31984E82B8899
	output2	5CE058EBA8BF7325D381E30E57E31560511EB2D25A94DA43A8AAAE10C6BD0ECB B1BC7F4757ED8DE7D40283F2F15B91DDEE31FE1593804D482FF8FFBC876FFCD5

7.4.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	375A1E76B3FA3443A9828311D271C3A54ED67057B68203B7C651C1C0CD394A6C E65A339CBD05A90FCB730FAB1121E891D66EEC3D509B0946C0FB524D64D08576 BA71E363140D693FBC8AB947BD325DEF5F0CA7F561EC4406A63A5077052BA590
	output2	DB11111458D96BA3ECC7CCE10BFC713EA0A45C6A5315327CE5E667478BF5E17A 1B82F33F08CD7413144B8CC3B024F299694196E9639CE1C4F464839C65758A78 B957DC2BA0B649DAA4F1DCDC869EA264EA864AAD3B27FDDEB294F696EC415AEA

7.4.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	372E04912F7BA6A5730163052140200 65A908DAA0DBA65FCD0C8EEF53996CF89 0A490068701489A07C37C50FC2BA3BF72F825E3772BE212B49F0D5E59CAE4FAA 8BA6016A7C1FD68F0FA23139FE9797F6CD5401D46C16DAB38D307DC706B649BA 3D79CB060FC4AE88F90305BACE1C6946B6D2BC492BC6831E354BACE8E538C5C9
	output2	4393CAB1B5D5B52D0729E358679FA87FCD188FE32ADDC94EBC68BC8B02339C35 DD4EF4C495ADAAA46AF15B77F348D9C630C2BC57A0ED6CD140C06F7BA4FAF00C C8366466E627EA4F340894B00466103882E61604B80EEFDD8C4E7BA05C552518 2FEC804E13F406F13703044E740C4CB8A420EDB2BF142B51AAD26164CA092DA2

7.5 시나리오 3-4 (개별화 문자열 미사용, 추가 입력 미사용)

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

7.5.1 SHA-224를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8F3E95103AA4278091DEF41FC93467D74E8D184AB3A8A6380B5E9E1D655FFDA5 ADF4A109DCEB129DD3C8F74FC1EC7416192AEA929CCE6713
	output2	B44DF843948C18195D6CECC6B724A500F23CD2D54065604EBDF506C65DF05560 AC7203A4BDB96353E92294DC903B00C04AB6904F6E788725

7.5.2 SHA-256을 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	489FDAFA23E07E3DDBE28DFA164C3906BB6FCAA98A33B933736111ABEAA94DE0 510CE950B32FD9C9E7167F0840ED17F725BEB80EC04BB368AE0042ECBE3372BA
	output2	C2B9D81D357D3E2A7405C141F1952AEF66BD51401BD8D021079871982A7B53A7 C99B8986EFCA1211EC8A884D35E11EC09575C291CC4E0B70DCE0DA264B4B4EFF

7.5.3 SHA-384를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	8F524F33435573DC932E54F1C258EFD303F202D46DA8336F97D058E5545F836C 2BCF1F7C53F8225F6D312468DB1B18C83ECF09ED5AAFB63556B273D16B9C9522 0463B006D069C61E4A40DF0E5CB4EC451D5B8ED989CCCA2B5A10E790FE0546D9
	output2	D250F906BA72AE65EB52ED8CD2454A7D13B9D485EB92BCE978254AAF9319ACD2 FA7526A39D0BA099AE9B8ED3A0A9B5B29CF8FEA2DFB99B8D8D088ED71FE839D5 84B79A14A273003FD15DDC1302DE74B4A4FBCDA368D092D7EA0F940423B8934D

7.5.4 SHA-512를 사용하는 HMAC_DRBG의 참조 구현값

출력결과	output1	6E5CABE47E9BF5F1018AE97545D1635152FF79053C98A9C56F8B9E8A5CEAF1D7 A82620536A38B55807BD1D444A0869F0656015E32C67BC27D5B658E611E36C74 F8ABD2E904160D42D2B92FE4859363DCB199A3148488C5936D28BBB106D5BBCC 4117F12A2C7D7AAF47B1DB857C92ECB7E5A4FAAE1C3BA353BEBC05D46EFB9429
	output2	E3BE7EF9EA7A47C59ECE743772CC8A3E2910087D3FD1924D2BA4AA6B6569FDB5 C67BB3C0BC0F1693572C01EE079B792FAAA8AEEE35D714D0D93ACD4E4C8AF71F 2C7C57778BF48BC5380FB37AB98750763E0410ADC715C6F002E6A7725FE89661 9DB83DB95B2F3CF03C0DFC72BDF458A0A480BF348FCEF9A5AFFE9F8566077DA5

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

[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-Part2	-	정보보호기반 (PG501)