Summary of Errata and Clarifications to the HDCP on HDMI Specification Rev 2.2

Page 8, insert the following definition under Section 1.2

> **Permitted Type 1 Audio Portion**. *Permitted Type 1 Audio Portion* consists of the audio portion of Audiovisual Type 1 Content Stream which is sampled at no more than 24 bits, with a sampling frequency of no more than 192 kHz and no more than 8 channels. Such audio portions may be transmitted by the HDCP Repeater to all HDCP Devices. The HDCP Repeater must support the transmission of Permitted Type 1 Audio Portions to HDCP-protected Interface Ports connected to HDCP Devices compliant with HDCP 2.2 or higher, if such ports are available at the HDCP Repeater.

Replace all references to HDCP2_0_REPEATER_DOWNSTREAM with HDCP2_LEGACY_DEVICE_DOWNSTREAM.

Page 22, replace first sentence under Section 2.5.1.1 with the following

> When an HDCP Receiver (including HDCP Repeater) is newly connected to the HDCP Repeater or disconnected from the HDCP Repeater, and the HDCP Repeater has already completed the authentication protocol with the upstream HDCP Transmitter, the HDCP Repeater must make the RepeaterAuth_Send_ReceiverID_List message available for the upstream HDCP Transmitter to read, assert the READY status bit and set the Message_Size register to the size of the RepeaterAuth_Send_ReceiverID_List message.

Page 23, replace third sentence in 2nd paragraph under Section 2.5.2 with the following

> Type 0 Content Stream (see Section 4.2.12) and Permitted Type 1 Audio Portion may be transmitted by the HDCP Repeater to all HDCP Devices.

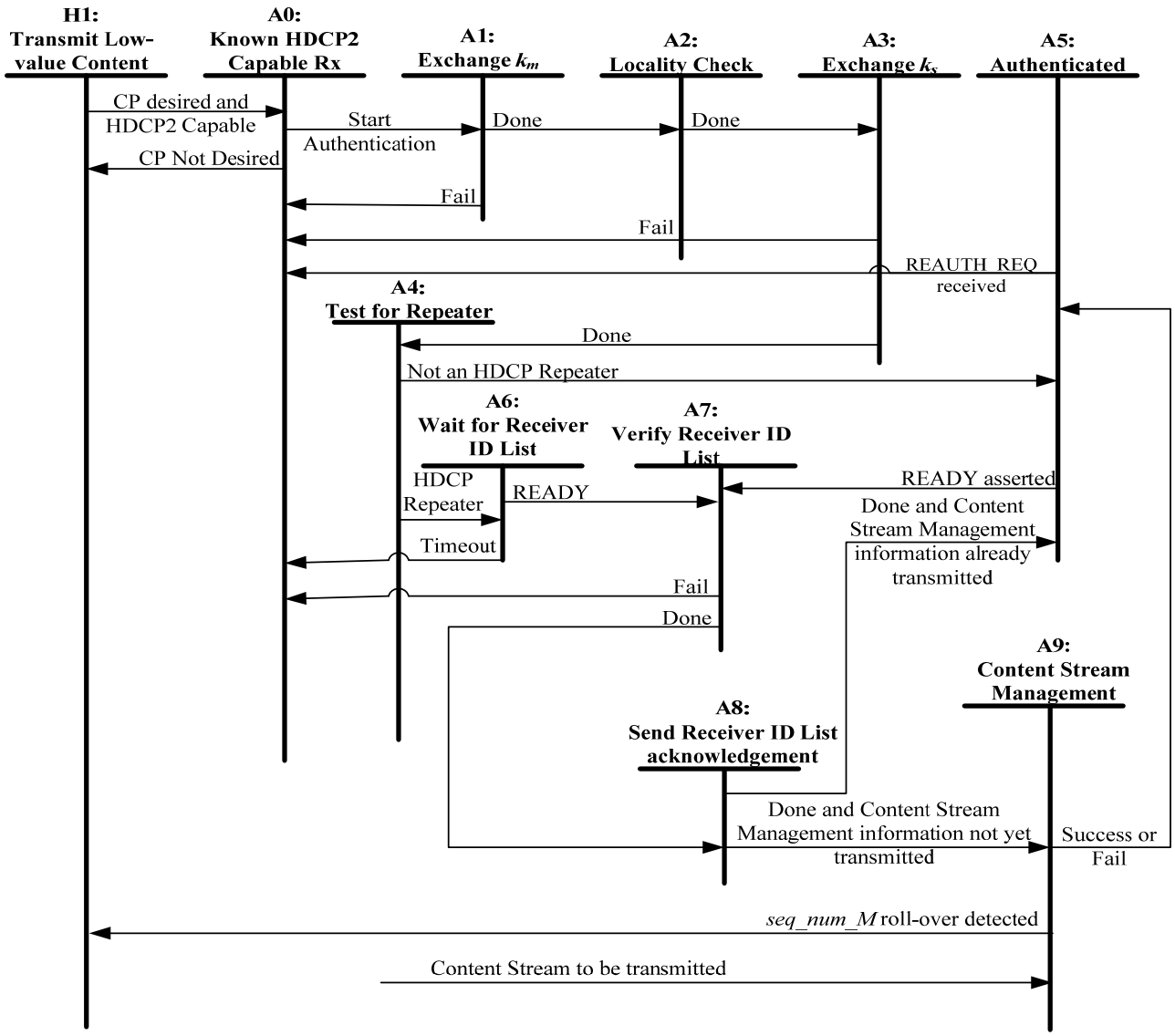
Page 23, replace last sentence in 2nd paragraph under Section 2.5.2 with the following

> Type 1 Content Stream (see Section 4.2.12), except Permitted Type 1 Audio Portion, must not be transmitted by the HDCP Repeater through its HDCP-protected Interface Ports connected to HDCP 1.x-compliant Devices, HDCP 2.0-compliant Devices and HDCP 2.1-compliant Devices.

Page 24, replace the 6th sentence in the 2nd paragraph under Section 2.6 with the following

> The HDCP Receiver must either assert the REAUTH_REQ bit of the RxStatus register or de-assert HDCP_HPD to the upstream transmitter once it determines loss of synchronization.

Page 27, replace Figure 2.12 in Section 2.8 with the following

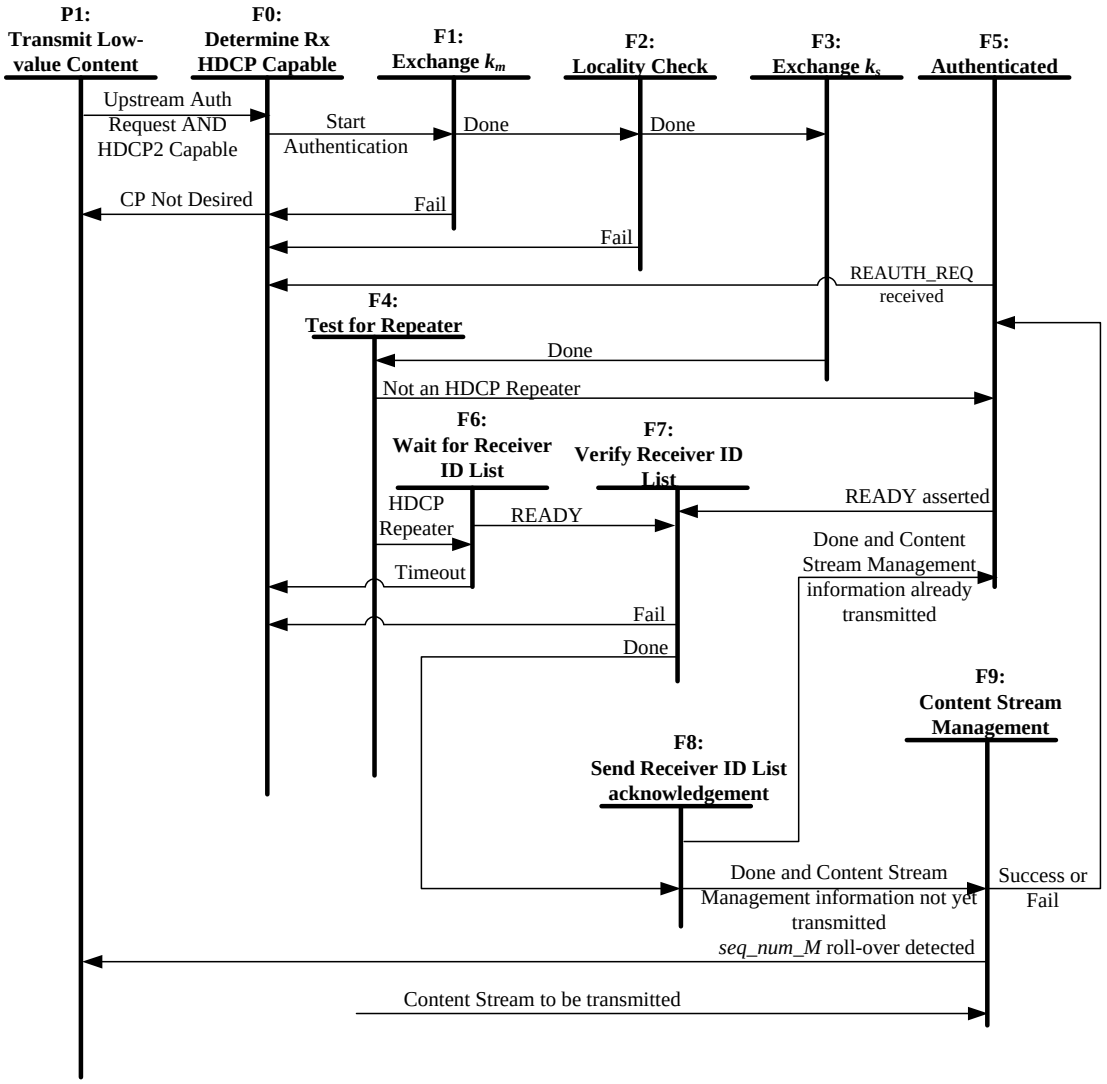


Page 30, insert the following state transition under Section 2.8

Transition A9:H1. This transition occurs if *seq_num_M* rolls over. *seq_num_M* must never be reused during an HDCP Session for the computation of M' (or M). If seq_num_M rolls over, the HDCP Transmitter must disable HDCP Encryption if encryption is enabled, restart authentication by the transmission of a new AKE_Init message.

Note: The addition of *seq_num_M* roll-over is not intended to support any mid-Content Stream Type value change.

Page 35, replace Figure 2.15 in Section 2.10.2 with the following

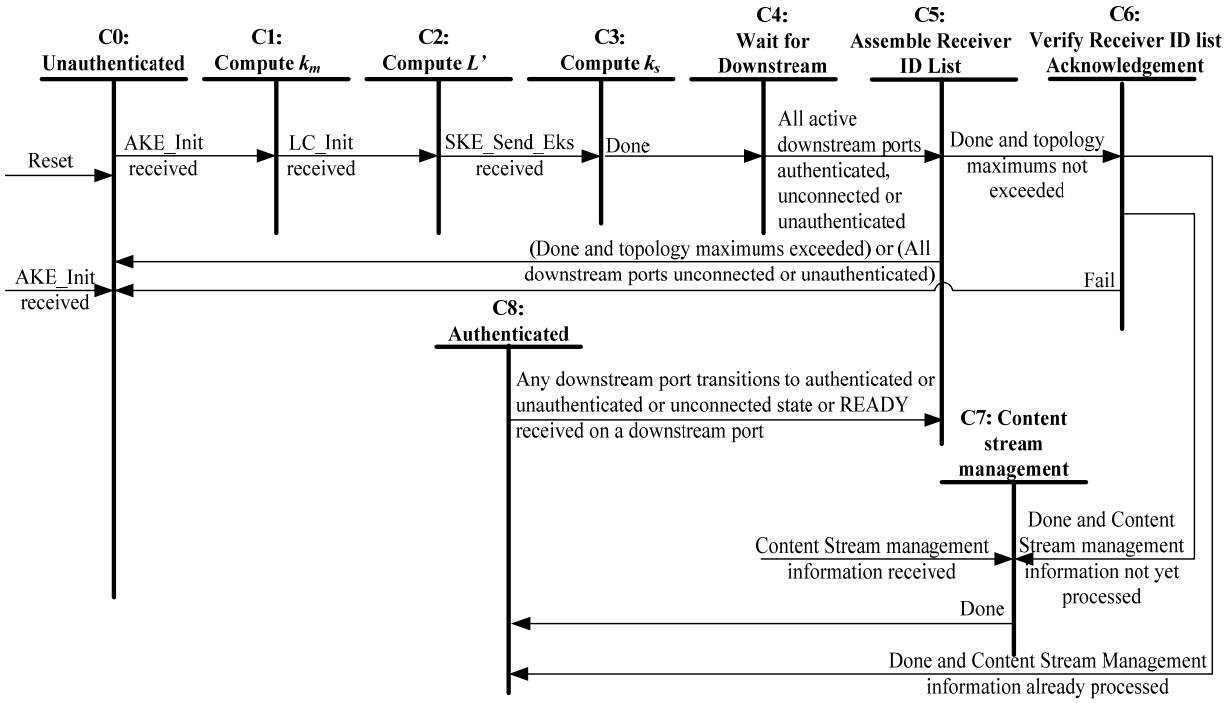


Page 38, insert the following state transition under Section 2.10.2

Transition F9:P1. This transition occurs if *seq_num_M* rolls over. *seq_num_M* must never be reused during an HDCP Session for the computation of M′ (or M). If *seq_num_M* rolls over, the downstream side must disable HDCP Encryption if encryption is enabled, restart authentication by the transmission of a new AKE_Init message.

Note: The addition of *seq_num_M* roll-over is not intended to support any mid-Content Stream Type value change.

Page 39, replace Figure 2.16 in Section 2.10.3 with the following



Page 39, replace 2nd sentence under State C0: Unauthenticated with the following

If a transition in to this state occurred from State C6 or from State C5, when State C5 is implemented in parallel with State C8, the upstream side must either set the REAUTH_REQ status bit in the *RxStatus* register or de-assert HDCP_HPD to the upstream transmitter.

Page 40, replace 11th paragraph with the following

If any downstream port connected to an HDCP Repeater detects the HDCP2_0_REPEATER_DOWNSTREAM or HDCP1_DEVICE_DOWNSTREAM bits read from the repeater to be set to one, the upstream side sets the corresponding bits to one in the *RxInfo* register which is read by the upstream HDCP Transmitter as part of the RepeaterAuth_Send_ReceiverID_List message.

Page 41, add the following paragraph under Transition C8:C5

This transition also occurs when a downstream port that was previously in an authenticated state transitions in to an unauthenticated or unconnected state. For example, the transition may occur when an active, authenticated HDCP Receiver attached to the downstream port is disconnected.

Page 46, replace the last sentence in the 1st paragraph under Section 2.14 with the following

The multi-byte value at offset address 0x70 (*RxStatus*) must be stored in little-endian format. Multi-byte values that are passed through the 1-byte Read_Message (at offset address 0x80) and Write_Message (at offset address 0x60) addresses, as part of the authentication protocol messages

(Section 4), must be transferred in big-endian format. For example, the values r_{tx} and *TxCaps* sent as part of the AKE_Init message, the values $cert_{rx}$, r_{rx} and *RxCaps* sent as part of the AKE_Send_Cert message, the value $E_{kpub}\_k_m$ sent as part of the AKE_No_Stored_km message are all sent in big-endian order.

Page 52, replace the first sentence in 3rd paragraph under Section 3.3 with the following

The CTLx signals described in Table 3.3 are only valid within a 16-clock window of opportunity starting at 512 TMDS character clocks following the active edge of VSYNC.

Page 53, replace the first sentence in the 4th paragraph with the following

It is required that no Data Island or Video Data, nor any Guard Band, be transmitted during a keep-out period that starts 508 TMDS character clocks past the active edge of VSYNC and ends 650 TMDS character clocks past the active edge of VSYNC.

Page 53, replace the first and second sentence in the 7th paragraph with the following

Video Data Periods begin with a two-character Leading Guard Band. The state transition variable videoData is defined to go TRUE on the TMDS character clock coinciding with the first active pixel (or portion of the pixel bits when the pixel bit depth is higher than 24 bits per pixel) of video data in the period (i.e. after the Guard Band) and is defined to go FALSE on the first TMDS character clock following the last active pixel of video data in the period. (NOTE: When the pixel bit depth is higher than 24 bits per pixel, a single pixel data straddles multiple TMDS character clock cycles.)

Page 53, replace the first sentence in the 8th paragraph with the following

Data Islands begin with a two-character Leading Guard Band and end with a two-character Trailing Guard Band.

Page 53, replace the last sentence in the 8th paragraph with the following

The state transition variable *packetData* is defined to go TRUE for the first TMDS character clock of the Data Island containing packet data (i.e. first TMDS character clock following the Leading Guard Band) and is defined to go FALSE following the last TMDS character clock containing packet data (i.e. the first TMDS character clock of the Trailing Guard Band).

Page 54, replace the 2nd paragraph with the following

The state transition signal AVMUTE is defined to be TRUE for a duration of one TMDS character clock coincident with

the assertion of ENC_EN or ENC_DIS if the HDCP Device is in an AVMUTE state, as defined in the HDMI Specification.

Page 55, replace the second and third sentence under State G1 with the following

Subsequently, the FrameNumber field of *inputCtr* is incremented and the DataNumber field of *inputCtr* is reset to 0(zero) at every ENC_EN; this new value for *inputCtr* must be ready within 118 TMDS character clocks after the assertion of ENC_EN. It is required that no Data Island or Video Data, nor any Guard Band, be transmitted during a keep-out period that starts 508 TMDS character clocks following VSYNC and ends 118 TMDS character clocks past the assertion of ENC_EN.

Page 59, replace 4th paragraph under Section 4.2.10 with the following

The HDCP Repeater sets *RxInfo*.HDCP2_LEGACY_DEVICE_DOWNSTREAM bit to one if an HDCP 2.0-compliant Device or HDCP 2.1-compliant Device is attached to any one of its downstream ports, else it sets *RxInfo*.HDCP2_LEGACY_DEVICE_DOWNSTREAM to zero.

Page 60, replace the row corresponding to HDCP2_0_REPEATER_DOWNSTREAM in Table 4.13 with the following

HDCP2_LEGACY_DEVICE_DOWNSTREAM	1	Rd	When set to one, indicates presence of an HDCP2.0-compliant Device or HDCP2.1-compliant Device in the topology

Page 61, replace Type decription in Table 4.16 with the following

0x00: Type 0 Content Stream. May be transmitted by the HDCP Repeater to all HDCP Devices.

0x01: Type 1 Content Stream. Except for Permitted Type 1 Audio Portion, must not be transmitted by the HDCP Repeater to HDCP 1.x-compliant Devices, HDCP 2.0-compliant Devices and HDCP 2.1-compliant Devices.

0x02 – 0xFF : Reserved for future use only. Content Streams with reserved Type values must be treated similar to Type 1 Content Streams

Page 68, Table A.1, delete rows corresponding to *V* and *V'* and insert the following rows to the table

V[255:128]	Yes	Yes	No	N/A
V'[127:0]	Yes	Yes	No	N/A
V[127:0]	No	No	No	N/A

V'[255:128]	No	No	No	N/A
M	Yes	Yes	No	N/A
M'	No	No	No	N/A

Page 72, replace "Pixel clk" in Figure D.1 with "TMDS character clk".

Add Appendix E to the specification as specified below.

Appendix E. Test Vectors

E.1 Facsimile Keys

Note: The facsimile keys provided must be used ONLY for test purposes.

All values are provided in big-endian order.

Table E.1 provides facsimile key information for transmitter T1.

	Value in Hex
Global Constant lc_{128}	93 ce 5a 56 a0 a1 f4 f7 3c 65 8a 1b d2 ae f0 f7

Table E.1

Table E.2 provides the facsimile public parameters associated with the DCP LLC key $kpub_{dcp}$. These parameters are used only for test purposes. They are not used in production devices or SRMs.

	Value in Hex
Modulus n	A2 C7 55 57 54 CB AA A7 7A 27 92 C3 1A 6D C2 31 CF 12 C2 24 BF 89 72 46 A4 8D 20 83 B2 DD 04 DA 7E 01 A9 19 EF 7E 8C 47 54 C8 59 72 5C 89 60 62 9F 39 D0 E4 80 CA A8 D4 1E 91 E3 0E 2C 77 55 6D 58 A8 9E 3E F2 DA 78 3E BA D1 05 37 07 F2 88 74 0C BC FB 68 A4 7A 27 AD 63 A5 1F 67 F1 45 85 16 49 8A E6 34 1C 6E 80 F5 FF 13 72 85 5D C1 DE 5F 01 86 55 86 71 E8 10 33 14 70 2A 5F 15 7B 5C 65 3C 46 3A 17 79 ED 54 6A A6 C9 DF EB 2A 81 2A 80 2A 46 A2 06 DB FD D5 F3 CF 74 BB 66 56 48 D7 7C 6A 03 14 1E 55 56 E4 B6 FA 38 2B 5D FB 87 9F 9E 78 21 87 C0 0C 63 3E 8D 0F E2 A7 19 10

	9B 15 E1 11 87 49 33 49 B8 66 32 28 7C 87 F5 D2 2E C5 F3 66 2F 79 EF 40 5A D4 14 85 74 5F 06 43 50 CD DE 84 E7 3C 7D 8E 8A 49 CC 5A CF 73 A1 8A 13 FF 37 13 3D AD 57 D8 51 22 D6 32 1F C0 68 4C A0 5B DD 5F 78 C8 9F 2D 3A A2 B8 1E 4A E4 08 55 64 05 E6 94 FB EB 03 6A 0A BE 83 18 94 D4 B6 C3 F2 58 9C 7A 24 DD D1 3A B7 3A B0 BB E5 D1 28 AB AD 24 54 72 0E 76 D2 89 32 EA 46 D3 78 D0 A9 67 78 C1 2D 18 B0 33 DE DB 27 CC B0 7C C9 A4 BD DF 2B 64 10 32 44 06 81 21 B3 BA CF 33 85 49 1E 86 4C BD F2 3D 34 EF D6 23 7A 9F 2C DA 84 F0 83 83 71 7D DA 6E 44 96 CD 1D 05 DE 30 F6 1E 2F 9C 99 9C 60 07
Public Exponent e	03

Table E.2

Table E.3 and Table E.4 provide the facsimile certificates ($cert_{rx}$) for receivers R1 and R2.

As provided in Table 2.1 of High-bandwidth Digital Content Protection System, Revision 2.2, Mapping HDCP to HDMI specification, the certificate format consists of 40-bit Receiver ID, followed by 1048-bit Receiver Public Key, 4-bit Reserved2, 12-bit Reserved1 and 3072-bit Signature fields. All values are stored in big-endian format.

For example, in Table E.3, 0x745bb8bd04 is the Receiver ID which is followed by Receiver Public Key, Reserved2, Reserved1 and Signature fields.

	Value (Sequence of Hexadecimal bytes) for R1
Certificate ($cert_{rx}$)	74 5b b8 bd 04 af b5 c5 c6 7b c5 3a 34 90 a9 54 c0 8f b7 eb a1 54 d2 4f 22 de 83 f5 03 a6 c6 68 46 9b c0 b8 c8 6c db 26 f9 3c 49 2f 02 e1 71 df 4e f3 0e c8 bf 22 9d 04 cf bf a9 0d ff 68 ab 05 6f 1f 12 8a 68 62 eb fe c9 ea 9f a7 fb 8c ba b1 bd 65 ac 35 9c a0 33 b1 dd a6 05 36 af 00 a2 7f bc 07 b2 dd b5 cc 57 5c dc c0 95 50 e5 ff 1f 20 db 59 46 fa 47 c4 ed 12 2e 9e 22 bd 95 a9 85 59 a1 59 3c c7 83 01 00 01 10 00 0b a3 73 77 dd 03 18 03 8a 91 63 29 1e a2 95 74

	42 90 78 d0 67 25 b6 32 2f cc 23 2b ad 21 39 3d 14 ba 37 a3 65 14 6b 9c cf 61 20 44 a1 07 bb cf c3 4e 95 5b 10 cf c7 6f f1 c3 53 7c 63 a1 8c b2 e8 ab 2e 96 97 c3 83 99 70 d3 dc 21 41 f6 0a d1 1a ee f4 cc eb fb a6 aa b6 9a af 1d 16 5e e2 83 a0 4a 41 f6 7b 07 bf 47 85 28 6c a0 77 a6 a3 d7 85 a5 c4 a7 e7 6e b5 1f 40 72 97 fe c4 81 23 a0 c2 90 b3 49 24 f5 b7 90 2c bf fe 04 2e 00 a9 5f 86 04 ca c5 3a cc 26 d9 39 7e a9 2d 28 6d c0 cc 6e 81 9f b9 b7 11 33 32 23 47 98 43 0d a5 1c 59 f3 cd d2 4a b7 3e 69 d9 21 53 9a f2 6e 77 62 ae 50 da 85 c6 aa c4 b5 1c cd a8 a5 dd 6e 62 73 ff 5f 7b d7 3c 17 ba 47 0c 89 0e 62 79 43 94 aa a8 47 f4 4c 38 89 a8 81 ad 23 13 27 0c 17 cf 3d 83 84 57 36 e7 22 26 2e 76 fd 56 80 83 f6 70 d4 5c 91 48 84 7b 18 db 0e 15 3b 49 26 23 e6 a3 e2 c6 3a 23 57 66 b0 72 b8 12 17 4f 86 fe 48 0d 53 ea fe 31 48 7d 86 de eb 82 86 1e 62 03 98 59 00 37 eb 61 e9 f9 7a 40 78 1c ba bc 0b 88 fb fd 9d d5 01 11 94 e0 35 be 33 e8 e5 36 fb 9c 45 cb 75 af d6 35 ff 78 92 7f a1 7c a8 fc b7 f7 a8 52 a9 c6 84 72 3d 1c c9 df 35 c6 e6 00 e1 48 72 ce 83 1b cc f8 33 2d 4f 98 75 00 3c 41 df 7a ed 38 53 b1

Table E.3

	Value (Sequence of Hexadecimal bytes) for R2
Certificate ($cert_{rx}$)	8b a4 47 42 fb e4 68 63 8a da 97 2d de 9a 8d 1c b1 65 4b 85 8d e5 46 d6 db 95 a5 f6 66 74 ea 81 0b 9a 58 58 66 26 86 a6 b4 56 2b 29 43 e5 bb 81 74 86 a7 b7 16 2f 07 ec d1 b5 f9 ae 4f 98 89 a9 91 7d 58 5b 8d 20 d5 c5 08 40 3b 86 af f4 d6 b9 20 95 e8 90 3b 8f 9f 36 5b 46 b6 d4 1e f5 05 88 80 14 e7 2c 77 5d 6e 54 e9 65 81 5a 68 92 a5 d6 40 78 11 97 65 d7 64 36 5e 8d 2a 87 a8 eb 7d 06 2c 10 f8 0a 7d 01 00 01 10 00 06 40 99 8f 5a 54 71 23 a7 6a 64 3f bd dd 52 b2 79 6f 88 26 94 9e af a4 de 7d 8d 88 10 c8 f6 56 f0 8f 46 28 48 55 51 c5 af a1 a9 9d ac 9f b1 26 4b eb 39 ad 88 46 af bc 61 a8 7b f9 7b 3e e4 95 d9 a8 79 48 51 00 be a4 b6 96 7f 3d fd 76 a6 b7 bb b9 77 dc 54 fb 52 9c 79 8f ed d4 b1 bc 0f 7e b1 7e 70 6d fc b9 7e 66 9a 86 23 3a 98 5e 32 8d 75 18 54 64 36 dd 92 01 39 90 b9 e3 af 6f 98 a5 c0 80 c6 2f a1 02 ad 8d f4 d6 66 7b 45 e5 74 18 b1 27 24 01 1e ea d8 f3 79 92 e9 03 f5 57 8d 65 2a 8d 1b f0 da 58 3f 58 a0 f4 b4 be cb 21 66 e9 21

	7c 76 f3 c1 7e 2e 7c 3d 61 20 1d c5 c0 71 28 2e b7 0f 1f 7a c1 d3 6a 1e a3 54 34 8e 0d d7 96 93 78 50 c1 ee 27 72 3a bd 57 22 f0 d7 6d 9d 65 c4 07 9c 82 a6 d4 f7 6b 9a e9 c0 6c 4a 4f 6f be 8e 01 37 50 3a 66 d9 e9 d9 f9 06 9e 00 a9 84 a0 18 b3 44 21 24 a3 6c cd b7 0f 31 2a e8 15 b6 93 6f b9 86 e5 28 01 1a 5e 10 3f 1f 4d 35 a2 8d b8 54 26 68 3a cd cb 5f fa 37 4a 60 10 b1 0a fe ba 9b 96 5d 7e 99 cf 01 98 65 87 ad 40 d5 82 1d 61 54 a2 d3 16 3e f7 e3 05 89 8d 8a 50 87 47 be 29 18 01 b7 c3 dd 43 23 7a cd 85 1d 4e a9 c0 1a a4 77 ab e7 31 9a 33 1b 7a 86 e1 e5 ca 0c 43 1a fa ec 4c 05 c6 d1 43 12 f9 4d 3e f7 d6 05 9c 1c dd

Table E.4

Table E.5 and Table E.6 provide the private keys for receivers R1 and R2.

	Value in Hex for R1
P	ec be e5 5b 9e 7a 50 8a 96 80 c8 db b0 ed 44 f2 ba 1d 5d 80 c1 c8 b3 c2 74 de ee 28 ec dc 78 c8 67 53 07 f2 f8 75 9c 4c a5 6c 48 94 c8 eb ad d7 7d d2 ea df 74 20 62 c9 81 a8 3c 36 b9 ea 40 fd
Q	be 00 19 76 c6 b4 ba 19 d4 69 fa 4d e2 f8 30 27 36 2b 4c c4 34 ab d3 d9 8c d6 b8 0d 37 5e 59 4b 76 70 68 2b 1f 4c 3d 47 5f a5 b1 cd 74 56 88 fe 7c f8 3b 30 6f fd c3 ed 87 3c a1 53 84 c3 d2 7f
d mod (p-1)	60 71 9b e9 e8 f3 97 1f fe 13 d4 bf 7a a2 0d f6 7b cf 3e aa 17 47 75 c3 7f ec d9 44 9e c9 6a 02 e9 e4 af 56 51 d5 47 a9 09 b2 c5 16 a7 8b 2b 34 a0 33 6e 2f 3d 95 7b e8 ef 02 e4 14 bf 44 28 d9
d mod (q-1)	10 0e 2e 18 ad 5d e4 43 fe 81 1e 17 aa d0 52 31 5e 10 76 a2 35 d9 37 43 b0 f5 0c 04 81 e3 45 24 6d 53 be 59 b6 81 58 c4 49 3e d5 31 89 5d 2e a2 62 a9 0f 47 5e 8f 51 19 27 4e 66 4b 8a 72 89 bd
q^-1 mod p	3e 53 0a f4 8e 75 e1 52 c6 24 e9 f7 bb ac 3f 22 5f e8 e0 79 35 ff 91 ee 22 56 d2 00 68 32 c4 e1 5f ff f8 b1 1d ee dc 57 81 d1 ab 8b 37 22 e3 9f d0 a1 c1 ce 1d d0 24 23 a0 0e f7 a6 db a3 ea d3

Table E.5

	Value in Hex for R2
P	f5 f6 fa 44 a2 16 2f a7 1f 7f 16 05 99 26 c4 1b 80 7f fa 52 4e 3e aa 3d 1e b0 f1 9a c6 3d 8f 57 2b 9e cd e8 03 d6 f3 91 75 e2 19 44 9e 11 58 5f d6 88 7c c4 c1 5b 45 9b 84 cf 72 1d 35 bf 24 d5
q	ed ba 08 bf 42 2c 0e fa 3a c4 d2 c7 01 51 25 ae b0 a1 cc db 67 9b aa 50 f0 80 ac 4b 9f 5c ba 1e f4 7f a9 b3 21 8b 62 2c 36 da cd a7 4d a4 d6 44 ed b1 34 e7 69 10 77 5a 6a ff f5 63 8a 2c 43 09
d mod (p-1)	61 5a c4 6c 6e 0b 82 09 10 3a 69 29 06 19 85 fd ac ba fb 05 a0 da c4 df 34 4a ad 16 a9 e8 ab d7 c0 f8 36 5f e3 45 2d 5b

	21 e1 c0 46 9c 9a 18 f4 b6 21 87 e1 08 f7 6b 71 c6 fb a5 1b 52 ae b9 91
d mod (q-1)	5a 83 7f bb 1a bd dd c2 06 c8 54 1c b3 72 ab 2f 55 4f 75 c9 80 2c 73 ef b7 72 b6 a7 60 79 14 e0 9e 65 51 3e c4 21 e6 f2 40 bc 94 9b 03 e4 24 35 40 6f 3d 5e 72 d1 73 30 39 17 55 de 5d 88 b6 c9
q^-1 mod p	bc 91 2a 93 6a 8d 24 3c d5 7d 12 3b a3 71 c7 3a f0 64 72 50 7e 18 71 e1 b4 3b 1e fc 38 ca e6 8c 16 51 97 d6 3f 04 ee 23 8b 45 0c 4b 98 36 18 27 29 1b 4d 73 7e e8 b0 1a c7 fb 5c ea 78 d0 6e 97

Table E.6

Table E.7 provides the global constant (lc_{128}) used for receivers R1 and R2. Note that the same global constant is used in T1, R1 and R2.

	Value in Hex for R1	**Value in Hex for R2**
Global Constant lc_{128}	93 ce 5a 56 a0 a1 f4 f7 3c 65 8a 1b d2 ae f0 f7	93 ce 5a 56 a0 a1 f4 f7 3c 65 8a 1b d2 ae f0 f7

Table E.7

E.2 Authentication Protocol

Table E.8 provides test vectors generated during the authentication protocol between T1-R1 and T1-R2. The values provided in the table are as generated or received on the transmitter (T1) side.

	Value in Hex for R1	**Value in Hex for R2**
Authentication and Key Exchange (Without stored k_m)		
r_{tx}	18 fa e4 20 6a fb 51 49	f9 f1 30 a8 2d 5b e5 c3
Receiver ID(Extracted from certificate $cert_{rx}$)	74 5b b8 bd 04	8b a4 47 42 fb
RxCaps	02 00 01 (Device is an HDCP Repeater, *RxCaps*.REPEATER is set to one)	02 00 00 (Device is not an HDCP Repeater, *RxCaps*.REPEATER is zero)
TxCaps	02 00 00	02 00 00
Certificate signature verification	Hash: 4d d6 ef 0f 5a dd d4 82 a8 ce bc 62 1d c3 b5 f0 50 f6 39 f1 d3 8b a6 a4 4f ca 58 4b 45 a9 e9 39 Encoded Message EM:	Hash: 08 fe 9c 34 64 c3 ca 9a 76 38 43 b0 61 4f 55 b4 db 7b 9b 3e c2 8f 72 09 04 0e 81 4e 5c 2e 75 bd Encoded Message EM: 00 01 ff ff ff ff

	00 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20 4d d6 ef 0f 5a dd d4 82 a8 ce bc 62 1d c3 b5 f0 50 f6 39 f1 d3 8b a6 a4 4f ca 58 4b 45 a9 e9 39	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20 08 fe 9c 34 64 c3 ca 9a 76 38 43 b0 61 4f 55 b4 db 7b 9b 3e c2 8f 72 09 04 0e 81 4e 5c 2e 75 bd
$kpub_{rx}$ (Extracted from certificate $cert_{rx}$)	n: af b5 c5 c6 7b c5 3a 34 90 a9 54 c0 8f b7 eb a1 54 d2 4f 22 de 83 f5 03 a6 c6 68 46 9b c0 b8 c8 6c db 26 f9 3c 49 2f 02 e1 71 df 4e f3 0e c8 bf 22 9d 04 cf bf a9 0d ff 68 ab 05 6f 1f 12 8a 68 62 eb fe c9 ea 9f a7 fb 8c ba b1 bd 65 ac 35 9c a0 33 b1 dd a6 05 36 af 00 a2 7f bc 07 b2 dd b5 cc 57 5c dc c0 95 50 e5 ff 1f 20 db 59 46 fa 47 c4 ed 12 2e 9e 22 bd 95 a9 85 59 a1 59 3c c7 83 e: 01 00 01	n: e4 68 63 8a da 97 2d de 9a 8d 1c b1 65 4b 85 8d e5 46 d6 db 95 a5 f6 66 74 ea 81 0b 9a 58 58 66 26 86 a6 b4 56 2b 29 43 e5 bb 81 74 86 a7 b7 16 2f 07 ec d1 b5 f9 ae 4f 98 89 a9 91 7d 58 5b 8d 20 d5 c5 08 40 3b 86 af f4 d6 b9 20 95 e8 90 3b 8f 9f 36 5b 46 b6 d4 1e f5 05 88 80 14 e7 2c 77 5d 6e 54 e9 65 81 5a 68 92 a5 d6 40 78 11 97 65 d7 64 36 5e 8d 2a 87 a8 eb 7d 06 2c 10 f8 0a 7d e: 01 00 01
k_m	68 bc c5 1b a9 db 1b d0 fa f1 5e 9a d8 a5 af b9	ca 9f 83 95 70 d0 d0 f9 cf e4 eb 54 7e 09 fa 3b
$E_{kpub}(km)$	Seed: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F lhash:	Seed: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F lhash: e3 b0 c4 42 98 fc

	e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55 $E_{kpub}(km)$: 9b 9f 80 19 ad 0e a2 f0 dd a0 29 33 d9 6d 1c 77 31 37 57 e0 e5 b2 bd dd 36 3e 38 4e 7d 40 78 66 97 7a 4c ce c5 c7 5d 01 57 26 cc a2 f6 de 34 dd 29 be 5e 31 e8 f 1 34 e8 1a 63 a3 6d 46 dc 0a 06 08 99 9d db 3c a2 9c 04 dd 4e d9 02 7d 20 54 ec ca 86 42 1b 18 da 30 9c c4 cb ac b4 54 de 84 68 71 53 6d 92 17 ca 08 8a 7a f9 98 9a b6 7b 22 92 ac 7d 0d 6b d6 7f 31 ab f0 10 c5 2a 0f 6d 27 a0	1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55 $E_{kpub}(km)$: a8 55 c2 c4 c6 be ef cd cb 9f e3 9f 2a b7 29 76 fe d8 da c9 38 fa 39 f0 ab ca 8a ed 95 7b 93 b2 df d0 7d 09 9d 05 96 66 03 6e ba e0 63 0f 30 77 c2 bb e2 11 39 e5 27 78 ee 64 f2 85 36 57 c3 39 d2 7b 79 03 b7 cc 82 cb f0 62 82 43 38 09 9b 71 aa 38 a6 3f 48 12 6d 8c 5e 07 90 76 ac 90 99 51 5b 06 a5 fa 50 e4 f9 25 c3 07 12 37 64 92 d7 db d3 34 1c e4 fa dd 09 e6 28 3d 0c ad a9 d8 e1 b5
r_{rx}	3b a0 be de 0c 46 a9 91	e1 7a b0 fd 0f 54 40 52
$dkey_0$	4f 14 8d 11 dd 49 18 10 6f ab 16 6f f6 fd a6 ed	2a 04 d7 eb 0a 0b 4e 20 26 45 84 01 1e ab 0a 4a
$dkey_1$	b5 02 0c 0d f2 81 ba df e4 19 77 fa d0 ac 61 17	f9 dc 18 97 e8 ee d8 f9 ec 6a 5d 34 a9 62 02 c9
k_d	4f 14 8d 11 dd 49 18 10 6f ab 16 6f f6 fd a6 ed b5 02 0c 0d f2 81 ba df e4 19 77 fa d0 ac 61 17	2a 04 d7 eb 0a 0b 4e 20 26 45 84 01 1e ab 0a 4a f9 dc 18 97 e8 ee d8 f9 ec 6a 5d 34 a9 62 02 c9
H	69 e0 ab 21 2f db 57 e6 7e fc 43 76 1a 2c 5c ce 76 c3 65 f1 9b 75 c3 ea c2 d2 77 dd 5c 7e 4a c4	4f f1 a2 a5 61 67 c8 e0 ad 16 c8 95 99 1b 1a 21 a8 80 c6 27 39 3f c7 bb 83 ed a7 e5 69 07 a5 dc
H'	69 e0 ab 21 2f db	4f f1 a2 a5 61 67

	57 e6 7e fc 43 76 1a 2c 5c ce 76 c3 65 f1 9b 75 c3 ea c2 d2 77 dd 5c 7e 4a c4	c8 e0 ad 16 c8 95 99 1b 1a 21 a8 80 c6 27 39 3f c7 bb 83 ed a7 e5 69 07 a5 dc
Pairing		
$E_{kh}(k_m)$	Hash of private = SHA256 hash on concatenation of p, q, d mod (p-1), d mod (q-1), q^-1 mod p i.e. SHA-256(p ||q||d mod (p-1)||d mod (q-1)||q^-1 mod p): db e7 c0 f2 32 e8 dd 33 43 00 c3 9b 20 57 7a da 85 86 c7 b6 6d 9f b3 66 a0 76 0c fb c2 ab 4d 34 k_h: 85 86 c7 b6 6d 9f b3 66 a0 76 0c fb c2 ab 4d 34 $E_{kh}(k_m)$: b8 9f f9 72 6a 6f 2c 1e 29 b6 44 8d dc a3 10 bd	Hash of private = SHA256 hash on concatenation of p, q, d mod (p-1), d mod (q-1), q^-1 mod p i.e. SHA-256(p ||q||d mod (p-1)||d mod (q-1)||q^-1 mod p): 8a da 77 4a e0 1b 26 f8 c8 9d e1 f3 23 fd e2 15 c6 aa 14 eb b0 35 4d 50 83 f5 de 74 2a 8c 1b a2 k_h: c6 aa 14 eb b0 35 4d 50 83 f5 de 74 2a 8c 1b a2 $E_{kh}(k_m)$: e6 57 8e bc c7 68 44 87 88 8a 9b d7 d6 ae 38 be
m	18 fa e4 20 6a fb 51 49 3b a0 be de 0c 46 a9 91	f9 f1 30 a8 2d 5b e5 c3 e1 7a b0 fd 0f 54 40 52
Locality Check		
r_n	32 75 3e a8 78 a6 38 1c	a0 fe 9b b8 20 60 58 ca
L	bc 20 92 33 54 91 c1 9e a4 de 8b 30 49 c2 06 6a d8 11 a2 2a b1 46 df 74 58 47 05 a8 b7 67 fb dd	f2 0f 13 6e 85 53 c1 0c d3 dd b2 f9 6d 33 31 f9 cb 6e 97 8c cd 5e da 13 dd ea 41 44 10 9b 51 b0
L'	bc 20 92 33 54 91 c1 9e a4 de 8b 30 49 c2 06 6a d8 11 a2 2a b1 46 df 74 58 47 05 a8 b7 67 fb dd	f2 0f 13 6e 85 53 c1 0c d3 dd b2 f9 6d 33 31 f9 cb 6e 97 8c cd 5e da 13 dd ea 41 44 10 9b 51 b0

Session Key Exchange		
k_s	f3 df 1d d9 57 96 12 3f 98 97 89 b4 21 e1 2d e1	f3 df 1d d9 57 96 12 3f 98 97 89 b4 21 e1 2d e1
r_{iv}	40 2b 6b 43 c5 e8 86 d8	9a 6d 11 00 a9 b7 6f 64
$dkey_2$	bf ed 5a cb 93 28 d4 56 a9 f5 2e 0e f3 36 75 f3	45 54 97 7d 85 5d a8 c0 2a de f8 90 95 02 7d 1a
$E_{dkey}(k_s)$	4c 32 47 12 c4 be c6 69 0a c2 19 64 de 91 f1 83	b6 8b 8a a4 d2 cb ba ff 53 33 c1 d9 bb b7 10 a9
Authentication with Repeaters		
Upstream Propagation of Topology Information		
Receiver ID_0	47 8e 71 e2 0f	N/A as R2 is not an HDCP Repeater
Receiver ID_1	35 79 6a 17 0e	
Receiver ID_2	74 e8 53 97 a2	
Receiver ID list	47 8e 71 e2 0f 35 79 6a 17 0e 74 e8 53 97 a2	
RxInfo *RxInfo* fields Rsvd DEPTH DEVICE_COUNT MAX_DEVS_EXCEEDED MAX_CASCADE_EXCEEDED HDCP2_0_REPEATER DOWNSTREAM HDCP1_DEVICE_DOWNSTREAM	02 31 Values in binary 0000_b 001_b 00011_b 0_b 0_b 0_b 1_b	
seq_num_V	00 00 00	
V	63 6d c5 08 4d 6c b1 0e 93 a5 28 67 0f 34 1f 88	
V'	bc cc 7d 16 e6 bc b9 02 60 08 1d f7 4a b4 5c 8a	
Downstream Propagation of Content Stream Management Information		
STREAM_ID	00	
Type	01	
seq_num_M	00 00 00	
StreamID_Type||*seq_num_M*	00 01 00 00 00	
SHA256(k_d)	1e 6c 5c a4 40 9a 66 a6 20 96 fe cd fc f3 f6 b0 45 e4 44 6b f5 45 c8 45 2b 4a ee 48 0c 53 c4 dd	
M'	dd 26 e9 52 6e 0e 1d 69 c8 84 e4 cc	

	c8 09 aa c7 71 e9 97 b5 61 89 09 6e 4d 94 24 c2 1b 64 58 c6	

Table E.8

Table E.9 provides an HDCP 2 facsimile SRM signed with the facsimile DCP LLC key in Table E.2. The SRM revokes Receiver IDs of receivers R1 and R2

Receiver IDs revoked	74 5b b8 bd 04, 8b a4 47 42 fb
SRM Version	00 01
SRM Value	91 00 00 01 01 00 01 91 00 80 00 00 74 5b b8 bd 04 8b a4 47 42 fb 17 07 e9 ea 61 ad b4 2e 9a 44 a9 1e 44 ba ab 6f 6b 37 27 50 bb 17 8e ad c5 7f e8 f5 21 b4 60 1e 54 80 da 2a 1a 59 f3 9d e3 98 54 43 24 70 ca 83 47 64 2d c6 26 6d 30 05 b4 ee 9b b6 69 a2 f3 7c 7d 13 cf f3 a7 c7 89 ef 50 0d 32 e1 d2 2c d1 b5 46 d6 36 44 25 52 65 06 b6 31 e7 26 d2 5c 1c 17 b7 26 6f 73 e5 8a 6e e9 db 00 27 70 11 bb 75 a0 49 30 ff 38 b3 d8 2d 03 c1 78 50 74 ca 60 aa 32 03 28 8d e4 a1 8c 62 2d f3 61 6c bf a1 9c ab b3 d7 e7 d6 dc 31 f6 74 1a ab c0 9c 6a 0a c2 65 e4 29 bd 4e 22 73 5a 2c c7 75 96 e9 7a 16 a6 70 6b 3c ba 50 60 5a 33 d5 d7 f2 76 5b 5e 2d 45 e2 0e f1 4c 6d 8d cf af 39 23 79 a5 fb ae cb 8f d8 de df db 24 20 52 10 74 ba 42 6f ad bb 3e 3a a5 ce 99 0d ff 41 a6 0f 60 7f ae 05 00 3c 2c f3 ba 5a 86 1b 04 7f 53 e5 e3 68 dc 6b 36 25 73 69 95 5d 15 37 d6 98 d6 6b a8 d0 35 37 2d 2f f1 53 90 aa 32 87 99 3b b7 33 48 0e ce e4 f1 d8 93 51 eb 98 92 e7 2d ac a2 32 fb e1 f9 f1 7d 92 26 37 5d 4c 0c f8 a2 11 4c 2a 49 b6 48 bc cc 44 01 06 cb 74 da 0d 70 fa 06 64 a6 54 e6 7c 65 34 ff 97 ed db 8a 8d 40 be fe 60 e5 0c bf 50 60 7b 16 71 bd ff c3 1b fb 15 a5 10 07 6a 5d 1a 6c fa 67 dc b3 cd a3 85 6e eb 77 5f 92 8f ee fb d5 34 58 72 b1 55
SRM Signature Verification	Hash: 3b 11 c9 ee f0 b6 ec 5b 68 34 b2 67 95 7c 2d 03 1d 83 0a d7 38 78 07 24 c9 14 c6 74 4e f6 70 b0 Encoded Message: 00 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20 3b 11 c9 ee f0 b6 ec 5b 68 34 b2 67 95 7c 2d 03 1d 83 0a d7 38 78 07 24 c9 14 c6 74 4e f6 70 b0

Table E.9

E.3 Encryption

Table E.10 provides test vectors covering two frames of HDCP Content. Each frame has two lines with eight pixels per line. The test vectors are generated at Transmitter T1 for Receiver R2.

Note that when ENC_EN occurs, the unused key strem bits produced by the HDCP Cipher are discarded.

	Plaintext video data to be encrypted	Video data after encryption at T1
Line 1, Pixel 1	R 59 G c0 B 3e	R 96 G 22 B ca
Line 1, Pixel 2	R 9e G e5 B fe	R d0 G 3d B 97
Line 1, Pixel 3	R 9a G f9 B 19	R f7 G 56 B 5f
Line 1, Pixel 4	R 5b G 5d B 6c	R 72 G 8f B d4
Line 1, Pixel 5	R 55 G dc B de	R de G 4f B 7d
Line 1, Pixel 6	R e5 G 87 B 63	R 81 G bd B 2c
Line 1, Pixel 7	R be G fc B c7	R 52 G 87 B fc
Line 1, Pixel 8	R a1 G b5 B 65	R 39 G d4 B b7
Horizontal Blank		
Line 2, Pixel 1	R 12 G 6b B 14	R 36 G 30 B 65
Line 2, Pixel 2	R 06 G 4a B 73	R f8 G 38 B 43
Line 2, Pixel 3	R f8 G bb B 15	R 32 G 17 B d8
Line 2, Pixel 4	R cc G e6 B 21	R 03 G fd B e4
Line 2, Pixel 5	R 87 G 95 B 78	R db G 36 B 41
Line 2, Pixel 6	R d2 G 03 B f7	R c4 G cf B ea
Line 2, Pixel 7	R 62 G 81 B 44	R 91 G 71 B 28
Line 2, Pixel 8	R 80 G d8 B 75	R 7f G 25 B a3
Vertical Blank		
Line 1, Pixel 1	R 56 G bf B 8a	R 3d G a8 B 58
Line 1, Pixel 2	R 2c G 26 B 03	R a5 G 2c B ea
Line 1, Pixel 3	R 88 G 43 B dc	R 77 G 71 B ae
Line 1, Pixel 4	R 1d G db B bd	R 2d G af B 0a
Line 1, Pixel 5	R e6 G 32 B 13	R 4c G fb B 63
Line 1, Pixel 6	R 36 G 34 B 24	R e9 G f7 B c7
Line 1, Pixel 7	R 48 G 82 B 8f	R cb G 36 B 2f
Line 1, Pixel 8	R 99 G b9 B db	R c7 G 7f B 68
Horizontal Blank		
Line 2, Pixel 1	R 9c G ac B 7b	R 03 G 94 B ab
Line 2, Pixel 2	R 40 G 11 B d0	R 22 G 93 B ed
Line 2, Pixel 3	R aa G 3c B e6	R 76 G 12 B 54
Line 2, Pixel 4	R e6 G e9 B ac	R df G e7 B a2
Line 2, Pixel 5	R 7a G d5 B 2e	R 18 G d7 B d0
Line 2, Pixel 6	R 94 G 1f B 35	R a2 G 46 B 7f
Line 2, Pixel 7	R a7 G 85 B 64	R e3 G 5d B 21
Line 2, Pixel 8	R f7 G 45 B 16	R 29 G 4a B a8

Table E.10