Summary of Errata and Clarifications to the HDCP 1.1 Specification

Add subsections to 2.2 (especially).
Page 9, 1st paragraph after 2.2: 2.2.1 First part of authentication protocol

Page 11, 1st paragraph: 2.2.2 Second part of authentication protocol

Section 2.2, paragraph 11 (4th paragraph on page 11)

After "reads the KSV list and V from the HDCP Repeater.", add:

If the size of the KSV list exceeds the capacity of the HDCP Transmitter, the authentication protocol is aborted.

Section 2.2, append to paragraph 13

If either MAX_CASCADED_EXCEEDED or MAX_DEVS_EXCEEDED status bits are set, the READY bit may be set by the repeater, or it may not set the READY bit and simply let the timeout occur in the HDCP Transmitter.

Page 12, Table 2-1, second row. The entry for the second row "From" column should be AKSV3 (not AKSV2). The entry for the second row "To" column should be "RDY1" (not RDY2).

Page 13, 2nd paragraph: 2.2.3 Third part of authentication protocol

Figure 2-4 Third part of the authentication protocol:
Add footnote for the two "2 seconds" texts:

- reading Ri synchronously every 128th frame is also acceptable in lieu of asynchronous polling every 2 seconds

Change Kj to Ki and Mj to Mi in two places in figure 2-4

In paragraph 17 of section 2.2, after "once every two seconds.", insert:
Synchronous reading of Ri every time it changes (every 128th frame) is also acceptable in lieu of asynchronous polling. (Synchronous reading in the frame prior to Ri update and shortly after 1 millisecond of the Ri update also provides a method of detecting frame counter mismatch between HDCP transmitter and HDCP receiver when either device does not support Enhanced Link Verification.)

Page 14, at the end of section 2.2, add the following note:
Note: An HDMI-capable HDCP Transmitter that has enabled AC (by writing 1 to ENABLE_1.1_FEATURES bit of Ainfo) may need to re-authenticate after sending an AVMUTE to the HDCP Receiver, since the HDCP Receiver may have ignored the HDMI General Control Packet that contained the Set_AVMUTE command, causing the loss of HDCP cipher synchronization.

Page 18, State A9: Read KSV List, append to the first paragraph: If the size of the KSV list exceeds the capacity of the HDCP Transmitter, the authentication protocol is aborted.

Page 18, section 2.4, replace the second paragraph with the following:

> The Fast Re-authentication capability indication alerts the HDCP Transmitter that it may re-authenticate by writing a new Aksv and An without first resetting the HDCP Receiver by powering off the TMDS buffers for 100 ms. When set to 1, or the receiver is HDMI capable, no reset is necessary, and the receiver is capable of starting a new authentication if it receives a new Aksv in the B0:B1, B1:B2, and B2:B1 transitions as well as the B0, B1, and B2 states. If set to zero and the receiver is not HDMI capable, it may be necessary to reset the receiver prior to writing Aksv, which, in TMDS applications, may be effected by the HDCP Transmitter by powering off the TMDS buffers for a period of 100 ms.

Page 20. Add new paragraph after the first paragraph in section 2.5.

NOTE: HDCP Repeaters that have no active downstream HDCP Devices must be considered. The HDCP Repeater may authenticate as an HDCP Receiver with Bcaps REPEATER bit set to 0 if it wishes to receive HDCP Content, but may not pass HDCP Content to downstream devices. If an HDCP Transmitter encounters a downstream HDCP Repeater reporting a zero DEVICE_COUNT and sends it HDCP Content, it must complete the second phases of authentication successfully, computing V over an empty KSV list.

Page 28: Append the following to the end of Bit 5: READY, KSV FIFO ready.
See states C0 and C2.
Page 30: In the paragraph just before Fig 2-11, replace the last two sentences with:

HDCP Devices must support multi-byte reads with auto-increment. For reads beginning with the KSV FIFO address, the bytes will increment through the KSV FIFO data. For all other reads, the bytes will increment through the port addresses, reading one byte for each offset. Auto-incremented sequential accesses that start before the KSV FIFO address and cross through the KSV FIFO address read only the first byte of the KSV FIFO and then continue incrementing through the HDCP port address space.

On pages 31, first paragraph continued from page 30, change “read only the first byte of the KSV FIFO” to “access only the first byte of the KSV FIFO”.

Page 30: last A in Fig 2-11 should be “A-bar”
Page 31: last A in Fig 2-13 should be “A-bar” and not dotted (should be solid)

Page 31, Section 2.7, first paragraph

After “is in an authenticated state.”, add:

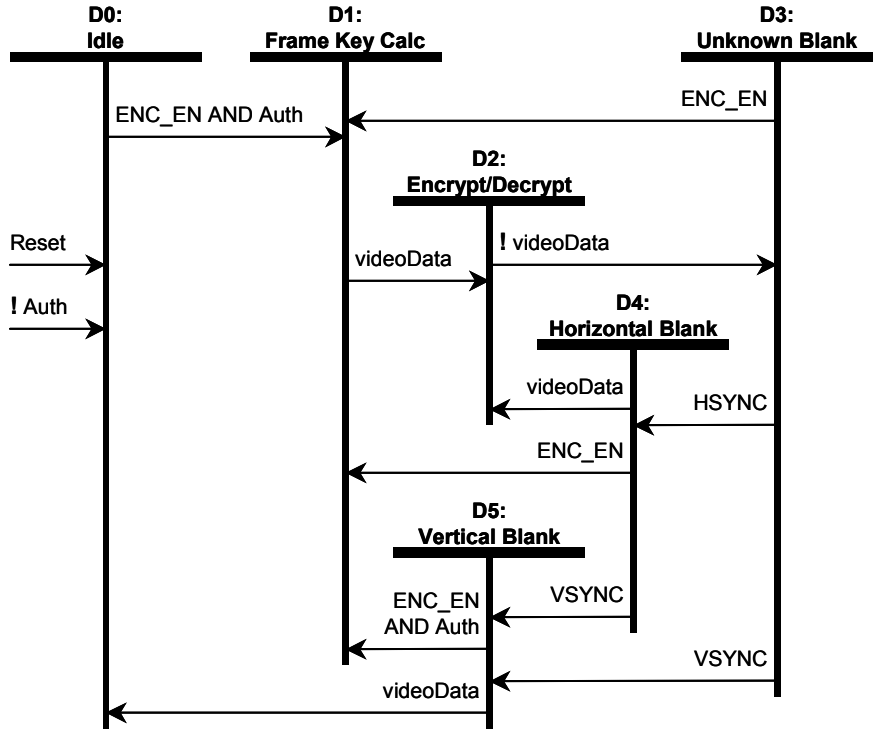
However, since an HDCP Transmitter may become unauthenticated with no immediate downstream indication, an HDCP Receiver may not be aware of this change and will continue to expect encryption signaling. Therefore it is highly recommended that the HDCP Transmitter not signal frame encryption while in the unauthenticated state. In the case of prior EESS signaling, it is recommended that the encryption-disabled signaling continue (rather than no encryption signaling), ensuring that the HDCP receiver properly displays the blue screen, informative display, or low value content which is sent while the HDCP Transmitter is in an unauthenticated state and the HDCP Receiver is still in an authenticated state.

Page 32: second paragraph, last sentence, change “bit 0 of the Ainfo register” to “the ENABLE_1.1_FEATURES bit of the Ainfo register”.

Page 32: third paragraph, last sentence, change “Ainfo bit 0” to “Ainfo bit ENABLE_1.l_FEATURES”.

Page 35: Enter new subsection 3.1.1 OESS right after 3.1 header

Page 35: Figure 3-2: replace by the HDCP 1.0 figure—OESS has not changed since enabling AC also enables EESS.

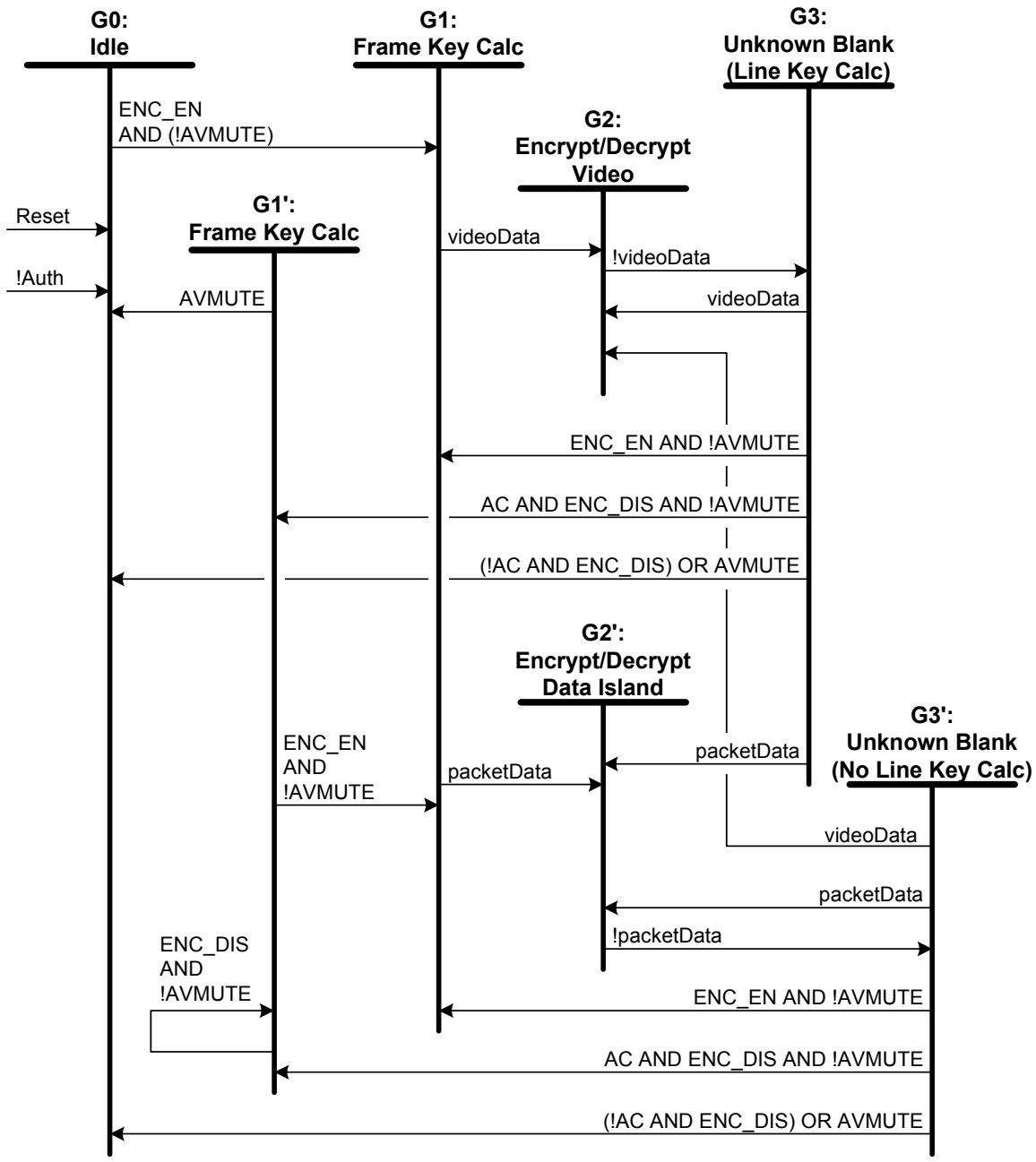


Page 36: remove sections State D1’: Frame Key Calculation, Transition D1’:D1, Transition D3:D1’.

Page 37: remove sections Transition D4:D1’, Transition D5:D1’.

Page 38: add new subsection 3.1.2 EESS at top of page

Page 39: replace figure 3-3 with corrected figure



Page 40: add new sections

State G1': Frame Key Calculation. The frame key for the next video frame is calculated as described in section 4.5, using hdcpBlockCipher. This state is only reached with the Advance Cipher option is enabled and an unencrypted frame is signaled.

Transition G1':G1. The assertion of Encryption Enable (ENC_EN) when in an authenticated state (as described in Section 2.7) causes frame key calculation.

Transition G1':G1'. The assertion of Encryption Enable (ENC_DIS) when in an authenticated state (as described in Section 2.7) causes frame key calculation.

Transition G1':G0. The detection of AVMUTE causes the encryption /decryption to enter the idle state.

Transitions G3:G1' and G3':G1'. In ADVANCE CIPHER mode the assertion of Encryption Disable (ENC_DIS) and not AVMUTE causes frame key calculation.

Page 47: Just before table 4-7, insert the following text:

For example, output bit 0 is computed as
(Bz17•Kz3) ⊕ (Bz26•Kz6) ⊕ (Bz22•Kz0) ⊕ (Bz27•Kz9) ⊕ (Bz21•Kz4) ⊕ (Bz18•Kz22) ⊕ (Bz2•Kz5) ⊕ By5 ⊕ Ky10.

Page 49: second paragraph: change ri to Ri.

Page 51: In the first paragraph, replace "Two acceptable methods are described in the HDCP Application note available from Digital Content Protection, LLC." by

That is, there must no way to determine the value--only change it from whatever it is to another value. For example, one can exclusive-or the influence values into the state. However, any 1-to-1 operation that does not reduce the number possible values or skew the otherwise uniform probability distribution of possible values is acceptable.

Add to the second paragraph:

This corresponds to about 40 (considering one million is about 2^20) random bits out of the 64 (or equivalent if the bits are biased).

Add a new paragraph:

An (incomplete) list of sources of entropy might include:
a) a true Random Number Generator or analog noise source, even if a poor (biased) one
b) a pseudo-random number generator (PRNG) where the state is stored in non-volatile memory after each use. (That is, every power on continues the sequence--it does produce not the same sequence each time). Flash memory or even disk is usable for this purpose as long as it is reasonably secure from tampering. The hdcpRngCipher combined with tamper-resistant non-volatile memory is one such solution.
c) timers, network statistics, error correction information, radio/cable television signals, disk seek times, etc.
d) Since the random number An is not used for secret material, a reliable (not manipulatable by the user) calendar and time-of-day clock can be used as a seed. For example, some broadcast content sources may give reliable date and time information.

Different product environments have different resources available to them. There is generally no one source that is available in all environments.

The initial state of the hdcpRngCipher is not defined and is left to the implementer. Ideally, one would prefer that the initial value be different for each device power-on, though this is not possible in many environments. In addition, the Rekey enable signal may but need not be enabled during hdcpRngCipher operation.

The An values do not have to be secret, but must be fresh. That is, the method of producing new values must have integrity.

While each An value is already required to be fresh, dual-link transmitters or transmitters with multiple downstream links must ensure that each downstream link receives a distinct An value for each link. This ensures that each link between HDCP devices that have multiple inputs or outputs sharing the same device keys will produce distinct session keys (Ks), encryption keystreams, and authentication values (Mi, Ri, Pj).

Page 52: Table 5-2 change row 2 column 3 text “number of device KSV’s in this list” to “number of KSV’s N in this list”
Change row 3 column 2 from “40” to “40 * N”

Page 77: add extended frame example test vectors for more frames.
Add SRM verification vectors.

```
Here are the intermediate results for a DSA signature verification of
the empty SRM in the specification table 5-1. This uses the real public
key in the specification in table 5-3.

Table A-26, empty SRM verification test vectors

message = 0x80, 0, 0, 1, 0, 0, 0, 0x2b
SHA-1 digest = e241fca6a4c634f1337e18b042d2f5fee7643c67
w = 4b5b63222239a1c0f40ca135ee5625048ff9d6ae
u1 = cee7d084a5356092cbde569ddb7587a75e9e47d4
u2 = a6ed36cacf4f02a627de1d27ed8a92083e023823
G^u1 =
147492f48e5351ddb71bd03f906759f06878d1f44580b8e1b0bed9c85bc0e2ab1a80f01
961b868fe3de271c6ca3ed536d368f6f55d100f44d4497319e7e57a4dd413dc32972331
0d08b40891bc29a130d0aab75c1c428b059f54aea62d4f220c6c14ca521a6141af7acb8
ee7aac68a6167a2270ebed875344979b88bfe63827b
Y^u2 =
c5d2c41ec216cc4ac1a07f6f6ad9caf504dc8cb71bf4f6e764e49bd6aec02c99a98f54a
55712fad3d86e56944ddad9ca6401c632948c5bbc9547078bf590b643f324b6d13c6a29
526f0d1d9ebfeb323f0d1c8f7109b75356963d227c6cb7fe4ce5f67fdadd6820696a27c
a9b2387b989d3384ab339f5521dc035f2ad09629cdc
product =
19eebd37c962302901b20dc529759b4d05a62b9602c97bae5a002e8c77178769e27f3ce
5ae5bdbd8427ebe0f7ace4288bae377f5cabca52c855b2f49d6e364186e636b6aa86f4a
5b4c7a8df0e1e174a7473469f00a438771c39fc735dd1f8b1e897bb798dea8df80287c0
9d5445e438bcca4c68313450f616c11858dd77869e1
v = d2489e49d057ae315b1abce00e4f6b92a6ba033b
```

Add extended Ri values as table A-27.

	REPEATER = 0				REPEATER = 1			
	A1 - B1	A1 - B2	A2 - B1	A2 - B2	A1 - B1	A1 - B2	A2 - B1	A2 - B2
R_0	8ae0	fb65	3435	4fd5	6485	3f68	dd9b	7930
R_1	6153	d543	8991	0488	ed21	6006	ccc3	e26b
R_2	d189	295a	0e1c	0659	97e0	dc65	960e	d9ff
R_3	2b74	1c17	20b0	e1a7	ec2b	32dd	7232	9ae9
R_4	2147	4315	0ac4	a809	f82a	5f01	1d5e	39da
R_5	2570	cc79	5412	b077	4167	3618	8cba	c0b7
R_{06}	9204	8d46	7f3d	52f4	03c3	a885	5271	4d40
R_{07}	9648	dac2	175c	b9ea	b900	fcf1	af20	426d
R_{08}	6b01	8255	3d2a	fe59	d672	669e	ad26	2464
R_{09}	6796	2642	2ba5	04b7	7ee6	3a5e	5510	627c
R_{10}	a193	8768	daa7	efaa	3d91	69b7	6654	c7c1
R_{11}	bffd	498b	57fd	8b58	b21b	ac84	10c3	8e5d
R_{12}	4b20	f41d	6d17	7dbf	77bf	e03f	5e54	5a04
R_{13}	85b8	6ab9	7a43	6b05	a95b	4778	3b2c	446b
R_{14}	f838	738e	f6a8	7fdf	36de	9d22	bf2c	0749
R_{15}	3e80	d655	f25c	8cb1	d19b	56b2	f389	0333
R_{16}	390f	9aff	ec0a	d3b9	3137	c601	31a6	94d5
R_{17}	2ecb	04f2	f4b8	857f	40d4	1eda	da43	8d22
R_{18}	c279	93a5	1ca8	3153	6586	bca0	0cd2	3c9d
R_{19}	596f	8f5d	169c	8fba	cfcb	2a18	1be6	5406

Table A-28. R_i values

Add table of Pj values (pixel value 0).

	A1 - B1		A1 - B2		A2 - B1		A2 - B2	
Frame	Ri	Pj	Ri	Pj	Ri	Pj	Ri	Pj
R_0	8ae0		fb65		3435		4fd5	
16		0xD1		0x8B		0x17		0x61
32		0x88		0xD9		0xB0		0x06
48		0xB4		0xA4		0x9C		0x41
64		0x38		0x68		0xF1		0xC2
80		0xA7		0x81		0x54		0xD0
96		0x4C		0x6A		0x3C		0x96
112		0xE4		0x61		0x34		0xB8
128	0x6153	0x53	0xD543	0x43	0x8991	0x91	0x0488	0x88
144		0x12		0x70		0xD8		0xFA
160		0x28		0x6F		0xE5		0x38
176		0x2D		0x05		0xA1		0x82
192		0xE1		0x6D		0xAA		0xF5
208		0xD5		0xB3		0x4C		0x11
224		0xF0		0xA2		0x7F		0xC0
240		0x92		0x97		0x1D		0x10
256	0xD189	0x89	0x295A	0x5A	0x0E1C	0x1C	0x0659	0x59

272		0xCD		0xA7		0x52		0xAD
288		0x9F		0x11		0x24		0xE1
304		0xB3		0x97		0x8D		0xF8
320		0x2F		0x7F		0xBF		0x58
336		0x49		0x10		0x44		0xE8
352		0x11		0x69		0xB6		0x0E
368		0x95		0xEF		0xC5		0x12
384	0x2B74	0x74	0x1C17	0x17	0x20B0	0xB0	0xE1A7	0xA7
400		0x45		0xE7		0xD6		0xF2
416		0x2C		0x57		0xF6		0x5F
432		0x07		0xF8		0xB6		0xB5
448		0xC8		0x5C		0xAC		0x09
464		0x4B		0x27		0x2C		0xBD
480		0x93		0xAF		0x14		0x5A
496		0xEF		0x6C		0xFE		0xE0
512	0x2147	0x47	0x4315	0x15	0x0AC4	0xC4	0xA809	0x09
528		0xE7		0x91		0x5D		0xE4
544		0x4C		0x29		0xC5		0xBB
560		0xDE		0xDA		0xE7		0xC3
576		0xD8		0x6C		0xB6		0xEB
592		0xC8		0x89		0xB4		0x3B
608		0xC3		0xB1		0x97		0x7E
624		0x05		0x38		0x53		0x62
640	0x2570	0x70	0xCC79	0x79	0x5412	0x12	0xB077	0x77

Table A-29. R_i and P_j values (REPEATER = 0)

Add table A-30 of Pj values for the repeater case.

	A1 - B1		A1 - B2		A2 - B1		A2 - B2	
Frame	**Ri**	**Pj**	**Ri**	**Pj**	**Ri**	**Pj**	**Ri**	**Pj**
R_0	6485		3f68		dd9b		7930	
16		0x73		0x88		0xE9		0xF9
32		0x32		0x03		0x1D		0x81
48		0xB3		0x24		0x97		0x73
64		0xCD		0x05		0xC0		0x3C
80		0x98		0x00		0x11		0xBC
96		0x18		0x00		0x25		0x21
112		0x97		0xA1		0x43		0x00
128	0xED21	0x21	0x6006	0x06	0xCCC3	0xC3	0xE26B	0x6B
144		0x8F		0x91		0x37		0x48
160		0x09		0xC6		0x5D		0x77
176		0x32		0xFF		0x11		0x18
192		0xEA		0xB3		0x14		0x1B
208		0xA5		0xB9		0x5E		0x3B
224		0xB7		0x10		0xFF		0xAF
240		0xED		0x03		0xC9		0xB6
256	0x97E0	0xE0	0xDC65	0x65	0x960E	0x0E	0xD9FF	0xFF
272		0x38		0x31		0x2F		0xB3
288		0x92		0xBF		0xC1		0x5C
304		0xC7		0x12		0x41		0x9D
320		0x5D		0x43		0x1B		0x7E
336		0x86		0xE9		0x04		0xA3
352		0x66		0xB6		0x20		0xC5
368		0x98		0xF9		0xE7		0x72
384	0xEC2B	0x2B	0x32DD	0xDD	0x7232	0x32	0x9AE9	0xE9
400		0xD8		0xB5		0xCF		0xED
416		0x80		0xAB		0xC7		0x45
432		0xA5		0xB2		0x27		0x09

448		0xE5		0x48		0xCA		0xAC
464		0xF8		0x6F		0xDA		0xFC
480		0x8C		0xEC		0xAE		0x32
496		0xB1		0x68		0x0D		0x2D
512	0xF82A	0x2A	0x5F01	0x01	0x1D5E	0x5E	0x39DA	0xDA
528		0x15		0x85		0xA4		0x45
544		0x66		0x07		0x95		0x4E
560		0xF0		0x63		0xC4		0x04
576		0xF6		0xE5		0xFD		0xC1
592		0x14		0x4A		0xF1		0xDD
608		0x8A		0x76		0xE0		0xA6
624		0xC1		0xFA		0x65		0xAB
640	0x4167	0x67	0x3618	0x18	0x8CBA	0xBA	0xC0B7	0xB7

Table C-3. R_i and P_j values (REPEATER = 1)

Page 78: Table B1 “Akeys” row change “Akeys” to “Akeys **”
In Bkeys row change “Bkeys” to “Bkeys **”

Add footnote to table B-1: “** KSV position excluded (see Aksv, Bksv)”

Change the row with value “Bx, By, Bx, Kx, Ky, Kz” to “Kx, Ky, Kz” and the size from 28 bits to 84 bits. (This is now consistent with the “Bx, By, Bz” row).