Kryptoanalyse des Premiere NDS Verschlüsselungssystem

Colibri
colibri_dvb@lycos.com
http://colibri.de.ms/
25. September 2008

Einleitung

Der Pay-TV Anbieter Premiere hat seit einiger Zeit auch neue sichere Smartcards von NDS im Einsatz. Die Receiver die kompatibel zu neuen NDS-Verschlüsselungssystem sind, wurden über Satellit auf die neue NDS-Firmware umgestellt.

Dies ist Grund genug eine Kryptoanalyse bei diesem, bei Premiere neuen, NDS System durchzuführen.

Gleich vorweg: Bis auf die DIREKT & Blue Movie Programme ist derzeit anscheinend eine Entschlüsselung aller Programme über die NDS-ECMs **ohne** Beteiligung einer Smartcard möglich.

Aber erstmal der Reihe nach.
Bei Premiere werden die Video und Audio Streams mit dem in Europa üblichen DVB-CSA-Algo [2] verschlüsselt. Dieser immer noch sichere Algo ist bereits seit einigen Jahren als Source Code verfügbar. Als Schlüssel wird ein 8 Byte (64 Bit) langer Wert, das sogenannte „Control Word“ (CW) verwendet. In der Praxis enthält das Control Word jedoch nie 8 zufällige Bytes sondern nur 6. Zwei Bytes werden aus den restlichen Bytes berechnet. Somit gibt es nur 2^{48} verschiedene Schlüssel.

Ein Control Word wird bei Premiere ca. alle 15 Sekunden geändert (Cryptoperiode). Ein bekannt gewordenes Control Word (wie weiter unten als echtes Beispiel aufgeführt) kann also nur Video und Audio für eben diese 15 Sekunden entschlüsseln die zeitgleich zu diesem einen Control Word übertragen worden sind.

Neben den verschlüsselten Video und Audio Streams müssen also die Control Words zum Receiver übertragen werden. Dazu ist ein eigener Pakettyp „Entitlement Control Message“ (ECM) vorgesehen. Daneben gibt es auch noch den Pakettyp „Entitlement Management Message“ (EMM). Diese EMM dienen z.B. dazu Updates auf Smartcards zu speichern.

Dieses Control Word wird natürlich nicht im Klartext über ein ECM übertragen, sondern verschlüsselt. Verwendet wird dazu der NDS-Algo, der einen Schlüssel verwendet, der auf allen freigeschalteten NDS-Smartcards von Premiere vorhanden und identisch ist. Dieser Schlüssel kann z.B. alle paar Monate über EMMs geändert werden.

Ein ECM hat u.a. zwei Bereiche. Einen IRD-ECM (IRD = Integrated Receiver Decoder) und einen Card-ECM Bereich. Der IRD-ECM Bereich wird vom Receiver selbst verarbeitet. Hier werden Infos wie z.B. Datum, Uhrzeit und Channel-ID übertragen. Die Infos im Card-ECM Bereich dagegen werden vom Receiver an die Smartcard weitergeleitet und von dieser verarbeitet. Hier ist auch das verschlüsselte Control Word enthalten. Jede freigeschaltete NDS-Smartcard von Premiere enthält den passenden Schlüssel und Algo zum Entschlüsseln

des Control Words. Mit diesem „Decrypted Control Word“ (DCW) kann der Receiver wiederum die Video und Audio Streams über den DVB-CSA-Algo entschlüsseln.
Soweit ist das Verfahren auch sicher. Denn wenn sich die NDS-Smartcard nicht hacken lässt, also die Schlüssel und Algos nicht auslesbar sind, ist das Verfahren sicher und keiner kann die Control Words entschlüsseln.

Bis hierher wäre alles so schon sicher gewesen. Aber was hat Premiere gemacht...

Premiere überträgt das Control Word mit einem anderen Schlüssel und Algo verschlüsselt ein zweites Mal zusätzlich im **IRD**-ECM Bereich. Diese Daten sind, wie oben beschrieben, für den Receiver selbst bestimmt und können von Ihm **ohne** Smartcard entschlüsselt werden.

Nur bei den Premiere DIREKT & Blue Movie Programmen wird **kein** zweites Control Word im IRD-ECM mit übertragen. Diese Programme sind also nur mit freigeschalteter Smartcard zu entschlüsseln. Bei allen anderen Programmen wird anscheinend ein zweites Control Word übertragen.

Das vorhanden sein des zusätzlichen Control Words ist offenbar kein versehentlicher Bug, sondern anscheinend Absicht.

Ob ein Receiver das zusätzliche Control Word auswertet kann Premiere anscheinend über ein EMM, das an die Seriennummer des Receivers gerichtet ist, steuern. Premiere kann somit Kunden, die mitteilen Ihre Smartcard funktioniert nicht mehr, eine neue Smartcard zuschicken und den Receiver z.B. für 14 Tage ohne Smartcard freischalten. Somit kann der Kunde solange die neue Smartcard noch nicht bei ihm angekommen ist, weiterhin Premiere schauen (zumindest ohne die DIREKT & Blue Movie Programme).

Dieses gravierende Sicherheitsproblem, das die sichere NDS-Smartcard „ad ab surdum“ führt, sollte Premiere schleunigst beheben und auf die zusätzliche Übertragung des zweiten Control Words verzichten. Premiere sollte darüber nachdenken, ob Sie den Kunden der eine nicht funktionierende Smartcard hat, nicht lieber eine Gutschrift über 14 Tage, die der Kunde das Programm nicht sehen kann, ausstellt.

Wie weiter unten gezeigt wird sind zur Entschlüsselung des Control Words nur Daten aus dem ECM und der Firmware nötig. Das schlimme ist das diese Firmware (zumindest für den Humax PR-HD1000 App-Version 1.00.39) unverschlüsselt über den Satelliten ausgestrahlt wird. Jeder mit einer DVBs Einsteckkarte für den PC kann neben dem Video, Audio und ECM Stream auch problemlos die Firmware aufzeichnen. Nach dem Auspacken liegt der Entschlüsselungsalgo offen. Für die Entschlüsselung benötigt der Algo neben 3 Parametern aus dem ECM auch zwei Parameter aus der Firmware. Auch diese zwei Parameter liegen unverschlüsselt in der Firmware offen rum.

Auch wird Premiere dringendst empfohlen die Firmwareupdates zukünftig nur noch verschlüsselt zu übertragen. Ein Loader im Receiver könnte dann die das Applikations-Update vor dem Abspeichern entschlüsseln.

Das Freischaltesignal für die smartcardlose Entschlüsselung wird anscheinend über ein EMM an den Receiver übertragen und im EEPROM gespeichert. Wie unten aus der Darstellung des Entschlüsselungsalgos zu entnehmen ist, fließen keinerlei Daten aus dem EMM in den Algo als Parameter mit ein. Besser wäre es im EMM zusätzlich Schlüsselmaterial, das in den Algo

als Parameter mit eingeht, mit zu übertragen. Dann könnte ein Hacker nicht einfach den Algo aus der Firmware extrahieren und ein Entschlüsselungsprogramm für den PC schreiben.

Ein weiteres Problem besteht darin, dass zwar in der Firmware ein paar Varianten der 40h Byte langen Parameter für den Entschlüsselungsalgo, die über ein Byte im ECM ausgewählt werden können, vorhanden sind, aber derzeit nicht genutzt werden (das Auswahlbyte war bis jetzt anscheinend immer 00h). Auch hier sollte Premiere diese Daten häufig wechseln um es den Hackern nicht unnötig leicht zu machen.

Im nächsten Kapitel wird das Sicherheitsproblem, die Control Word Berechnung ohne Smartcard anhand eines konkreten Beispiels verdeutlicht.

Control Word Berechnung ohne Smartcard

Die Control Word Berechnung soll anhand eines echten Beispiels gezeigt werden.
Die Beispielpakete stammen aus einer Aufzeichnung vom 16.09.2008 vom Transponder 11798H. Das verschlüsselte Audio (PID 200h) Paket und das passende ECM Paket (PID 1B42h) stammen vom Programm Premiere 1.

ECM Paket:

```
47 5B 42 16 00 80 70 87 00 00 01 1C 38 10 7E 6A 01 2D AA 55 05 10 0F 40 00 FF 8E 44 20 DD FF
3D 55 00 00 00 00 03 00 40 66 7E 0A 44 C1 32 CE DA 14 D6 41 00 00 90 58 C0 01 A6 02 C4 31 F5
7F 8E 70 40 C5 98 83 18 F4 49 25 92 AD 40 CA 37 A5 C5 98 E6 25 29 37 32 3C C6 0C BA 90 7E 03
06 ED 25 99 1C 90 8F FB DF 88 D5 4D C4 24 64 9A 78 F7 20 78 9C 3C F4 9A 90 E4 5B 16 C0 B8 3A
0A 80 12 C4 43 40 53 A7 DA 89 AE 97 C2 A2 F3 A7 25 25 16 FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF
```

Ein NDS ECM Packet enthält u.a. zwei Teile – den IRD-ECM (gelb) und Card-ECM Block (grau). Das erste Byte eines Blocks (1Ch bzw. 66h) enthält die Länge der zum Block gehörenden Daten. Normalerweise ist das Control Word nur im Card-ECM Block enthalten. Der Card-ECM Block wird zur Smartcard geschickt. Diese entschlüsselt das Control Word und sendet es zum Receiver zurück. Ohne Smartcard ist also üblicherweise keine Entschlüsselung möglich. Bei Premiere ist das aber zurzeit anders. Premiere sendet das mit einem einfacheren Algo verschlüsselte Control Word zusätzlich im IRD-ECM Block mit. Der IRD-ECM Block ist nicht für die Smartcard bestimmt, sondern er wird vom Receiver selbst verarbeitet.

Somit ist ein Premiere Receiver mit NDS Firmware in der Lage auf Befehl (über ein EMM Packet das an die Seriennummer des Receivers gerichtet ist) auf die smartcardlose Entschlüsselung umzuschalten. Dies kann nützlich sein, wenn jemanden meldet dass seine Smartcard defekt ist. Premiere kann dann, bis die Ersatzkarte beim Anwender eintrifft, die smartcardlose Entschlüsselung aktivieren.

Die smartcardlose Entschlüsselung funktioniert prinzipiell wie folgt:

IRD-ECM Block ohne Längenbyte:

```
38 10 7E 6A 01 2D AA 55 05 10 0F 40 00 FF 8E 44 20 DD FF 3D 55 00 00 00 00 03 00 40
```

Der Receiver fügt 4 Teilblöcke zu einem großen Block zusammen.
Teil 1: `38 10 7E 6A 01 2D AA 55 05 10` (das ist ein Ah langer Block aus dem ECM oben)
Teil 2: `00 00 00 03` (das ist ein 4 Byte langer Block aus dem ECM oben)
Teil 3: `85 81 E4 ...` (das ist ein 40h Byte langer Block aus der Firmware)

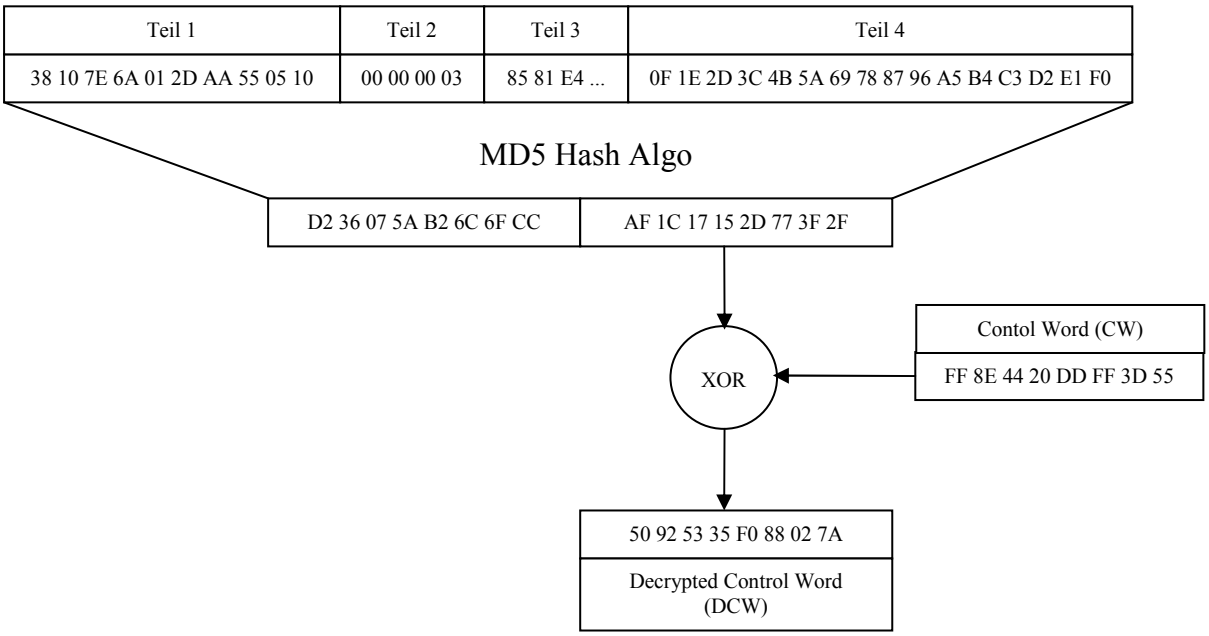
Teil 4: 0F 1E 2D 3C 4B 5A 69 78 87 96 A5 B4 C3 D2 E1 F0 (das ist ein 10h Byte langer Block aus der Firmware. Die HI-Nibbles in aufsteigender Reihenfolgen 0..Fh und die LO-Nibbles in Absteigender Reihenfolge Fh..0)

Dieser große (5Eh Byte lange) Block wird mit dem Hashalgo MD5 gehasht.
38 10 7E 6A 01 2D AA 55 05 10 00 00 00 03 85 81 E4 ... 0F 1E 2D 3C 4B 5A 69 78 87 96 A5 B4 C3 D2 E1 F0
Daraus entsteht folgender 16 Byte lange Hashwert:
D2 36 07 5A B2 6C 6F CC AF 1C 17 15 2D 77 3F 2F

Vom 16 Byte großen MD5 Hash wird nur die zweite 8 Byte große Hälfte benötigt:
AF 1C 17 15 2D 77 3F 2F
Dieser 8 Byte große Hash Wert wird mit dem verschlüsselten Control Word aus dem ECM hellblau dargestellt XOR verknüpft. Das Ergebnis ist das entschlüsselte Control Word (DCW).

```
    FF 8E 44 20 DD FF 3D 55 Verschlüsseltes Control Word (CW)
XOR AF 1C 17 15 2D 77 3F 2F Hashwert
------------------------------------------------------------
 =  50 92 53 35 F0 88 02 7A Entschlüsseltes Control Word (DCW)
    ========================
```

Control Word Algo:



Das entschlüsselte Control Word (DCW) kann nun dazu verwendet werden die Nutzdatenstreams (Video/Audio) zu entschlüsseln. Dies geschieht über den **nicht** Premiere spezifischen DVB-CSA-Algo [2].

Das DCW muss dazu, wie immer beim Einsatz vom DVB-CSA-Algo, von 64 Bit auf 48 Bit effektive Schlüssellänge geschwächt werden.
Dazu wird zuerst der Inhalt vom 3ten und 7ten Byte verworfen (64 – (2*8) = 48 Bit) und anschließend aus der Summe der der Bytes (0..2) bzw. (4..6) beschrieben.

```
CW[3] = CW[0] + CW[1] + CW[2];
CW[7] = CW[4] + CW[5] + CW[6];
```

In diesem Beispiel gibt es zwar keine Änderung im DCW, trotzdem muss es immer berechnet werden:

```
DCW vorher: 50 92 53 35 F0 88 02 7A
Berechnung: 50 + 92 + 53 = (1)35 / F0 + 88 + 02 = (1)7A
DCW nachher: 50 92 53 35 F0 88 02 7A
```

Dann wird der DVB-CSA-Algo mit dem DCW und dem verschlüsselten (Video oder Audio) Packet aufgerufen und heraus kommt das entschlüsselte Paket:

DCW:

```
50 92 53 35 F0 88 02 7A
```

Verschlüsseltes Audio Packet (PID 200h):

```
47 42 00 97 30 50 E2 F8 45 AB 68 16 25 E0 AD B5 65 5C 67 F4 7B 2F 0D F4 53 65 D8 C6 2B FB FA
D8 EF AD 7E 0C 4B 9F BD 07 68 27 7C 07 9C 37 A5 7D DD B7 BF 34 06 2F 5D 8A F8 E0 BD 33 21 7A
3C E2 FC 40 F0 FF DF 67 CF 5A 20 9D D5 78 0A 84 AE 26 AC 18 73 BE 4F 31 F9 D5 1E CC 76 EC CE
E7 64 4B DE 3B 9F 8E 0A AA 87 C4 6A BD 8E A9 30 B3 5E FD 3A 53 25 83 5D A9 DF B5 7A 17 52 C7
70 05 40 B0 DE CC 3B A3 68 D8 F8 99 D7 4F 29 F9 3A 8E 37 A0 72 8B 52 11 5A B4 BD F8 5E 96 D0
65 2B 2F F6 D9 AB 6A B5 0C 68 8A 68 9C 5F A8 65 4D 09 DD 7F 08 1C EE 33 2E 62 F6 79 CC 5E 61
99 53
```

Entschlüsseltes Audio Packet:

```
47 42 00 17 00 00 01 C0 0D 88 84 80 05 2B D4 FB 19 FD FF FC A4 00 9D F4 33 22 22 32 32 32 32
32 32 32 32 69 A6 92 49 44 89 24 90 00 00 00 BA AA AA FB AA AA AA C8 88 48 86 59 72 07 E1 86
28 A3 8E 28 E3 A2 3A 25 96 69 66 9E 79 E7 A2 8A 27 A6 9A A7 AA 7A A8 A6 9A 29 A6 9A 68 AA BA
29 BA 9A AD AE BA AC A6 BA EC 43 24 32 71 38 63 AD 42 D2 40 A5 0D 1C 55 1C 36 D3 E4 DB 9B 5C
A6 DB E4 9D 10 D3 C9 A6 2E 35 E1 2F 16 3C 3E 7D 6B 67 2A 50 A3 89 BB 76 44 DB 51 B6 DF 28 DE
B8 E1 A0 D9 C4 9F B6 9F 33 69 46 93 67 2C CB 2E 46 EC C7 8E FA BE 17 87 06 0C E5 EF 6B 66 E6
AA A2
```

Dass die Entschlüsselung geklappt hat kann man in diesem Fall gut an den gültigen MPEG-Header (00 00 01) des Audiostreams erkennen.

Welche Programme sind betroffen?

Folgende Programme sind von dem Problem betroffen, sie haben alle das zusätzliche Control Word im IRD-ECM Block. Dargestellt sind die Programmnummer (SID), der Programmname und das IRD-ECM (ohne Längenbyte). Erkennen kann man ein zusätzliches Control Word wenn an Position 08h das Bit0 gesetzt ist (das ist bei allen hier gezeigten Werten 05h/81h der Fall) und wenn an Position 09h das Bit4 gesetzt ist (das ist bei dem hier gezeigten Wert 10h auch der Fall). Das Control Word ist gelb dargestellt.

		Position	*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*
PrgNr:	9	Premiere 4	38	10	7E	6A	01	30	AA	55	05	10	0F	40	00	0F	9E	54	3F	7E	66	42	A7	00	00	00	00	03	00	F1
PrgNr:	10	Premiere 1	38	10	7E	6A	01	2D	AA	55	05	10	0F	40	00	FF	8E	44	20	DD	FF	3D	55	00	00	00	00	03	00	40
PrgNr:	11	Premiere 2	38	10	7E	6A	01	2E	AA	55	05	10	0F	40	00	D3	2C	15	0E	32	BF	6D	89	00	00	00	00	03	00	EB
PrgNr:	12	Animal Planet	38	10	7E	4D	00	CD	AA	55	05	10	0F	40	00	33	FF	D5	03	02	72	58	4D	00	00	00	00	03	00	86
PrgNr:	13	Discovery Geschichte	38	10	7E	4D	00	CE	AA	55	05	10	0F	40	00	0D	75	24	4C	AA	0E	5D	F0	00	00	00	00	03	00	5B
PrgNr:	14	Discovery Channel	38	10	7E	4D	00	CC	AA	55	05	10	0F	40	00	85	20	02	44	45	26	F1	27	00	00	00	00	03	00	D0
PrgNr:	15	Focus Gesundheit	38	10	7E	4D	00	CF	AA	55	05	10	0F	40	00	CE	D5	50	AA	EB	68	17	25	00	00	00	00	03	00	91
PrgNr:	16	Serie	38	10	7E	6A	01	31	AA	55	05	10	0F	40	00	CC	39	73	12	ED	2B	6D	C4	00	00	00	00	03	00	B8
PrgNr:	17	Sportportal	38	10	7E	33	00	68	AA	55	05	10	0F	40	00	44	A9	90	2D	BD	1C	B6	47	00	00	00	00	03	00	64
PrgNr:	19	Junior	38	10	7E	4D	00	CB	AA	55	05	10	0F	40	00	02	06	0C	81	53	80	85	B0	00	00	00	00	03	00	FE
PrgNr:	20	Filmfest	38	10	7E	33	00	66	AA	55	05	10	0F	40	00	EE	08	5A	91	62	B7	66	3D	00	00	00	00	03	00	7F
PrgNr:	22	Heimatkanal	38	10	7F	13	01	F8	AA	55	05	10	0F	40	00	91	84	6B	0E	C7	A8	A1	17	00	00	00	00	03	00	0B
PrgNr:	23	Krimi	38	10	7E	6A	01	32	AA	55	05	10	0F	40	00	7A	B7	0B	F3	70	5E	C6	AC	00	00	00	00	03	00	55
PrgNr:	27	RTL Crime	38	10	7F	14	01	F5	AA	55	05	10	0F	40	00	0E	8B	F5	E4	E8	92	43	28	00	00	00	00	03	00	AB
PrgNr:	28	Jetix	38	10	7E	4D	00	CA	AA	55	05	10	0F	40	00	F0	DB	4A	5C	62	47	05	48	00	00	00	00	03	00	C7
PrgNr:	29	Passion	38	10	7F	14	01	F6	AA	55	05	10	0F	40	00	A7	86	8D	D4	8C	EE	DD	FF	00	00	00	00	03	00	39
PrgNr:	34	Disney Channel	38	10	7E	4D	00	C9	AA	55	05	10	0F	40	00	E8	89	53	7D	02	87	72	7F	00	00	00	00	03	00	1A
PrgNr:	36	Sci Fi	38	10	7E	F6	01	95	AA	55	05	10	0F	40	00	3C	EE	A3	AE	37	3D	37	A4	00	00	00	00	03	00	9F
PrgNr:	41	Filmclassics	38	10	7E	33	00	65	AA	55	05	10	0F	40	00	D0	02	58	FD	4C	0A	83	A8	00	00	00	00	03	00	89
PrgNr:	42	13th Street	38	10	7E	F6	01	94	AA	55	05	10	0F	40	00	AA	8D	74	43	86	81	E4	25	00	00	00	00	03	00	D2
PrgNr:	43	Premiere 3	38	10	7E	6A	01	2F	AA	55	05	10	0F	40	00	C3	1D	E2	46	27	A6	A4	8E	00	00	00	00	03	00	EA
PrgNr:	50	1-2-3 TV	38	10	7F	13	01	FA	AA	55	05	10	0F	40	00	CC	69	44	8F	95	2F	31	B8	00	00	00	00	03	00	0D
PrgNr:	60	Kinowelt TV	38	10	7E	98	04	4E	AA	55	05	10	0F	40	00	48	AD	68	CC	94	EF	AC	84	00	00	00	00	03	00	0F
PrgNr:	61	TCM Deutschland	38	10	7E	98	04	4F	AA	55	05	10	0F	40	00	B3	88	F4	30	39	BC	62	61	00	00	00	00	03	00	4B
PrgNr:	62	AXN Deutschland	38	10	7E	98	04	50	AA	55	05	10	0F	40	00	CE	87	4F	52	5F	92	20	EC	00	00	00	00	03	00	28
PrgNr:	63	Romance TV	38	10	7E	98	04	51	AA	55	05	10	0F	40	00	1A	9D	7A	80	86	94	F9	26	00	00	00	00	03	00	20
PrgNr:	64	Playhouse Disney	38	10	7E	98	04	52	AA	55	05	10	0F	40	00	F3	57	6A	AB	B9	3E	AA	D1	00	00	00	00	03	00	08
PrgNr:	65	Toon Disney or Sat. 1 Comedy	38	10	7E	98	04	53	AA	55	05	10	0F	40	00	FE	39	28	83	79	7F	05	19	00	00	00	00	03	00	30
PrgNr:	66	Boomerang or Kabel 1 Classics	38	10	7E	98	04	54	AA	55	05	10	0F	40	00	24	56	EC	DA	D9	9F	50	57	00	00	00	00	03	00	98
PrgNr:	67	E clips	38	10	7E	98	04	55	AA	55	05	10	0F	40	00	97	AF	58	04	04	3F	37	56	00	00	00	00	03	00	AC
PrgNr:	150	Deutsche Charts	38	10	7F	14	02	01	AA	55	81	10	0F	40	00	11	0A	87	2A	E9	0C	8D	C9	00	00	00	00	03	00	F4

```
PrgNr:  151                 Rock Hymnen 38 10 7F 14 02 02 AA 55 81 10 0F 40 00 CB 2D 36 B3 52 78 52 CC 00 00 00 00 03 00 A7
PrgNr:  152                  Love Songs 38 10 7F 14 02 03 AA 55 81 10 0F 40 00 9F 77 E6 C9 C6 64 0C 7B 00 00 00 00 03 00 55
PrgNr:  153                   60er/70er 38 10 7F 14 02 04 AA 55 81 10 0F 40 00 31 C1 42 03 8A 25 9C 14 00 00 00 00 03 00 76
PrgNr:  154                   80er/90er 38 10 7F 14 02 05 AA 55 81 10 0F 40 00 23 06 48 23 15 B5 BF 76 00 00 00 00 03 00 74
PrgNr:  155                 R&B/Hip Hop 38 10 7F 14 02 06 AA 55 81 10 0F 40 00 65 C1 B5 A8 5E 25 36 B7 00 00 00 00 03 00 D5
PrgNr:  156                     Country 38 10 7F 14 02 07 AA 55 81 10 0F 40 00 54 E5 9B 70 C1 F4 5B 4A 00 00 00 00 03 00 81
PrgNr:  168                      Hit 24 38 10 7F 13 01 F9 AA 55 05 10 0F 40 00 3B 87 CF 6C F5 F7 3C FA 00 00 00 00 03 00 76
PrgNr:  221           Premiere Sport 1 38 10 7E 4D 00 D2 AA 55 05 10 0F 40 00 53 65 EB 70 C4 4F 0B 9E 00 00 00 00 03 00 37
PrgNr:  222           Premiere Sport 2 38 10 7E 33 00 6D AA 55 05 10 0F 40 00 7E 55 AB 3F E2 FC 6B 70 00 00 00 00 03 00 5F
PrgNr:  513              Erotik Ab 18! 38 10 7E F6 01 92 AA 55 05 10 0F 40 00 9F F1 43 F8 E4 E9 92 C4 00 00 00 00 03 00 C0
PrgNr:  515            The MGM Channel 38 10 7E F6 01 96 AA 55 05 10 0F 40 00 E9 7E 0B 1B C5 ED 40 12 00 00 00 00 03 00 67
PrgNr:  516         Premiere Nostalgie 38 10 7E 33 00 67 AA 55 05 10 0F 40 00 37 D7 5B 2B B5 86 54 C4 00 00 00 00 03 00 CA
PrgNr:  518               GoldStar TV 38 10 7F 13 01 F7 AA 55 05 10 0F 40 00 87 B4 48 07 32 D5 9F 6A 00 00 00 00 03 00 EF
PrgNr:  773                     BD 4 38 10 7F 40 02 C3 AA 55 05 10 0F 40 00 95 DC BE 15 C6 3A 30 B9 00 00 00 00 03 00 7C
PrgNr:13105                  NASN (P) 38 10 81 15 05 DD AA 55 05 10 0F 40 00 AC C4 81 E4 11 38 08 6A 00 00 00 00 03 00 D3
PrgNr:13203         Animax Deutschland 38 10 80 80 05 79 AA 55 05 10 0F 40 00 89 E2 61 BF 96 9B D9 6E 00 00 00 00 03 00 4C
PrgNr:13204            Cartoon Network 38 10 80 80 05 7A AA 55 05 10 0F 40 00 D5 AE 0A FF 8E DE 9B 2D 00 00 00 00 03 00 0A
PrgNr:13205               Eurosport 2 38 10 80 80 05 7B AA 55 05 10 0F 40 00 6F 7B 0C BA 8D 4D 12 18 00 00 00 00 03 00 FF
PrgNr:13207                RTL Living 38 10 80 80 05 7C AA 55 05 10 0F 40 00 2C 98 97 0B 04 D0 FE 55 00 00 00 00 03 00 D9
PrgNr:17505              Sat.1 Comedy 38 10 80 B7 03 85 AA 55 05 10 0F 40 00 57 CA 3C B7 9C 4B 16 B7 00 00 00 00 03 00 52
PrgNr:17506          kabel 1 classics 38 10 80 B7 03 86 AA 55 05 10 0F 40 00 9D 8C D8 C5 F6 DE 19 80 00 00 00 00 03 00 BE
PrgNr:28671                MTV Music 38 10 7E CA 04 B1 AA 55 05 10 0F 40 00 AA 2F 41 29 0F 1D 33 B5 00 00 00 00 03 00 1F
PrgNr:28681        MTV Entertainment 38 10 7E CA 04 B2 AA 55 05 10 0F 40 00 CB ED EC FC BE 2E 37 D3 00 00 00 00 03 00 5F
PrgNr:28682             Nick Premium 38 10 7E CA 04 B3 AA 55 05 10 0F 40 00 E1 17 35 12 12 8D AB AB 00 00 00 00 03 00 FE
```

Folgende Programme sind von dem Problem nicht betroffen, sie haben alle kein zusätzliches Control Word im IRD-ECM Block. Dargestellt sind die Programmnummer (SID), der Programmname und das IRD-ECM (ohne Längenbyte).

```
                              Position 00 01 02 03 04 05 06 07 08 09 0A
PrgNr:  665                  Blue Movie 38 10 7F 13 01 FC AA 55 04 00 E6
PrgNr:  666             Blue Movie Extra 38 10 7F 13 01 FD AA 55 04 00 E7
PrgNr:  671               Blue Movie Gay 38 10 7F 13 01 FE AA 55 04 00 E8
PrgNr:  208          Premiere Direkt 5 + 38 10 7E F6 01 97 AA 55 80 00 DF
PrgNr:  209            Premiere Direkt 4 38 10 7E F6 01 98 AA 55 80 00 E0
PrgNr:  220            Premiere Direkt 1 38 10 7E 33 00 6C AA 55 80 00 F0
PrgNr:  224          Premiere Direkt 1 + 38 10 7E 6A 01 33 AA 55 80 00 EF
PrgNr:  225            Premiere Direkt 5 38 10 7E 6A 01 34 AA 55 80 00 F0
PrgNr:  226            Premiere Direkt 3 38 10 7E 4D 00 D3 AA 55 80 00 71
PrgNr:  227          Premiere Direkt 2 + 38 10 7E 4D 00 D4 AA 55 80 00 72
PrgNr:  228          Premiere Direkt 1 + 38 10 7E F7 01 99 AA 55 80 00 E2
PrgNr:  242          Premiere Direkt 4 + 38 10 7E 33 00 69 AA 55 80 00 ED
PrgNr:  243            Premiere Direkt 3 38 10 7E 33 00 6A AA 55 80 00 EE
PrgNr:  244            Premiere Direkt 2 38 10 7E 33 00 6B AA 55 80 00 EF
PrgNr:  778              Direkt Erotik 1 38 10 7F 13 01 FF AA 55 80 00 65
PrgNr:  780              Direkt Erotik 2 38 10 7F 13 02 00 AA 55 80 00 67
```

Links:

[1] NDS FAQ by Colibri (darin wurde zwar damals das englische BSkyB NDS analysiert, das Premiere NDS ist vom Format her aber ähnlich aufgebaut) http://colibri.de.ms/

[2] DVB-CSA-Algo http://de.wikipedia.org/wiki/Common-Scrambling-Algorithmus