



- (51) **International Patent Classification:**
H04L 9/00 (2006.01) *G06F 21/55* (2013.01)
- (21) **International Application Number:**
PCT/IB2012/057428
- (22) **International Filing Date:**
18 December 2012 (18.12.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/632,877 1 February 2012 (01.02.2012) US
- (71) **Applicant (for all designated States except US):** **NDS LIMITED** [GB/GB]; One London Road, Staines Middlesex TW18 4EX (GB).
- (72) **Inventors; and**
- (71) **Applicants :** **GOLD, Martin** [GB/GB]; Shawford Dene, Shawford, Winchester Hampshire SO21 2BP (GB). **MILLAR, Keith** [GB/GB]; Gander House, 31 Gander Hill, Haywards Heath W.Sussex RH16 1QU (GB). **CAIN, Harel** [IL/IL]; 2 Esther Hamalka Street, 93627 Jerusalem (IL). **WACHTFOGEL, David** [IL/IL]; 20/10 Efrata Street, 93384 Jerusalem (IL). **DEVIR, Michal** [IL/IL]; 19

Harav Nissim Street, Kiryat Shmuel, 26383 Haifa (IL). **BERMAN, Max** [IL/IL]; Neve-Ilan, 90850 D.N.Harei Yehudah (IL). **WALZER, Brett** [IL/IL]; Box 304, 90917 Givat Zeev (IL).

(74) **Agents:** **KATZ, Samuel M.** et al.; NDS Legal (Patents), NDS Limited, One London Road, Staines Middlesex TW18 4EX (GB).

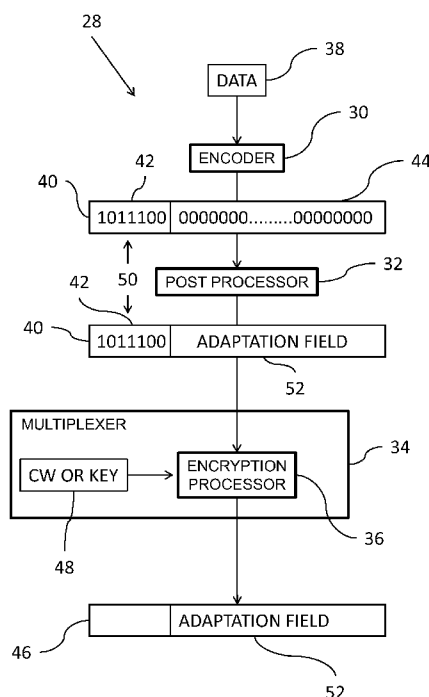
(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

[Continued on next page]

(54) **Title:** KNOWN PLAINTEXT ATTACK PROTECTION

Fig. 3



(57) **Abstract:** A Headend system including a encoder to encode input data yielding a plurality of data packets, each of the packets having a header and a payload, a post encoding processor to identify ones of the data packets having a payload with a suspected known plaintext, and modify at least some of the identified packets, and an encryption processor to encrypt at least some of the data packets yielding encrypted data packets. Related apparatus and methods are also described.



TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, **Published:**

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,

LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,

GW, ML, MR, NE, SN, TD, TG).

— *with international search report (Art. 21(3))*

KNOWN PLAINTEXT ATTACK PROTECTION

FIELD OF THE INVENTION

The present invention relates to protection against known plaintext attacks.

5

BACKGROUND OF THE INVENTION

The following references are believed to represent the state of the art:

Article entitled "Breaking DVB-CSA" by Erik Tews, Julian Walde, and Michael Weiner published in the conference record of the West European
10 Workshop on Research in Cryptography, Weimar, Germany, July 20-22, 2011;
and

A discussion in a forum at techrepublic.com/forum/discussions/102-276629.

15

SUMMARY OF THE INVENTION

The present invention, in certain embodiments thereof, seeks to provide an improved system for protection against plaintext attacks.

There is thus provided in accordance with an embodiment of the present invention, a system including an encoder to encode input data yielding a plurality of data packets, each of the packets having a header and a payload, a post encoding processor to identify ones of the data packets having a payload with a suspected known plaintext, and modify at least some of the identified packets, and an encryption processor to encrypt at least some of the data packets yielding encrypted data packets.

Further in accordance with an embodiment of the present invention, the post encoding processor is operative to modify the payload of the at least some identified packets so that the payload of each of the at least some identified packets is no longer a suspected known plaintext, and the encryption processor is operative to encrypt the data packets yielding the encrypted data packets.

Still further in accordance with an embodiment of the present invention, the post encoding processor is operative to replace at least some of the data of the payload of each of the at least some identified packets with random or pseudo-random data.

Additionally in accordance with an embodiment of the present invention, the post encoding processor is operative to replace at least some of the data of the payload of each of the at least some identified packets with other broadcast data.

Moreover in accordance with an embodiment of the present invention, the other broadcast data is selected from at least one of an entitlement management message (EMM), an entitlement control message (ECM), electronic program guide data, event information table (EIT) data, non-zero audio data, non-zero video data and metadata for the audio data or the video data.

Further in accordance with an embodiment of the present invention, the post encoding processor is operative to remove the payload of the at least some identified packets so that the payload of each of the at least some identified packets no longer exists, and for each one of the at least some identified packets, add an adaptation field to the one identified packet or lengthen a pre-existing adaptation field of the one identified packet, and the encryption processor is operative to encrypt the data packets having the payload yielding the encrypted data packets but not to encrypt the data packets without the payload.

Still further in accordance with an embodiment of the present invention, the post encoding processor is operative to reduce the length of the payload of each of the at least some identified packets to less than a certain length, and add an adaptation field to each of the at least some identified packets or lengthen a pre-existing adaptation field of each of the at least some identified packets, and the encryption processor is operative to encrypt the data packets having the payload with a length greater than or equal to the certain length yielding the encrypted data packets but not encrypt the data packets having the payload with a length less than the certain length.

Additionally in accordance with an embodiment of the present invention, the certain length is equal to eight bytes.

Moreover in accordance with an embodiment of the present invention, each of the bytes of the payload with the known plaintext is only selected from a value of zero and FF.

Further in accordance with an embodiment of the present invention, the input data encoded by the encoder is video data.

Still further in accordance with an embodiment of the present invention, the post encoding processor is operative to compare the payload of each of the data packets with at least one suspected known plaintext in order to identify the data packets having the payload with a suspected known plaintext.

Additionally in accordance with an embodiment of the present invention, the post encoding processor is operative to search the payload of each of the packets in order to find packets with matching payloads, select packets from

the matching payload packets where the same payload repeats in accordance with at least one frequency requirement, and assign the selected packets as suspected known plaintext packets.

Moreover in accordance with an embodiment of the present invention, the encryption processor is operative to encrypt the at least some data packets in accordance with a plurality of cryptoperiods and a plurality of keys such that a different one of the keys is used to encrypt the data packets in a different one of the cryptoperiods, and the at least one frequency requirement is that there could potentially be matching payload packets having the same payload at least once in each of the cryptoperiods.

Further in accordance with an embodiment of the present invention, the encoder is operative to add a continuity counter to the header of each of the packets, and the post encoding processor is operative to change the continuity counter of at least some of the packets to compensate for the modification of the at least some identified packets.

There is also provided in accordance with still another embodiment of the present invention, a method including encoding input data yielding a plurality of data packets, each of the packets having a header and a payload, identifying ones of the data packets having a payload with a suspected known plaintext, modifying at least some of the identified packets, and encrypting at least some of the data packets yielding encrypted data packets.

There is also provided in accordance with still another embodiment of the present invention, a system including an encoder to encode input data yielding a plurality of data packets, each of the packets having a header and a payload, a post encoding processor to search the payload of each of the packets in order to find packets with matching payloads, select packets from the matching payload packets where the same payload repeats in accordance with at least one frequency requirement, and assign the selected packets as suspected known plaintext packets.

Still further in accordance with an embodiment of the present invention, at least some of the data packets will be encrypted in accordance with a

plurality of cryptoperiods and a plurality of keys such that a different one of the keys is used to encrypt the data packets in a different one of the cryptoperiods, and the at least one frequency requirement is that there could potentially be matching payload packets having the same payload at least once in each of the
5 cryptoperiods.

There is also provided in accordance with still another embodiment of the present invention, a method including encoding input data yielding a plurality of data packets, each of the packets having a header and a payload, searching the payload of each of the packets in order to find packets with matching
10 payloads, selecting packets from the matching payload packets where the same payload repeats in accordance with at least one frequency requirement, and assigning the selected packets as suspected known plaintext packets.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

5 Fig. 1 is a partly pictorial, partly block diagram view of a Headend system encoding and encrypting data;

 Fig. 2 is a partly pictorial, partly block diagram view of a known plaintext attack against the Headend system of Fig. 1;

 Fig. 3 is a partly pictorial, partly block diagram view of a Headend
10 system with known plaintext attack protection constructed and operative in accordance with a first embodiment of the present invention;

 Fig. 4 is a partly pictorial, partly block diagram view the Headend system of Fig. 3 operating in accordance with an alternative mode of operation;

 Fig. 5 is a partly pictorial, partly block diagram view of the
15 Headend system of Fig. 3 in accordance with another alternative mode of operation; and

 Fig. 6 is a partly pictorial, partly block diagram view of an encoding and post processing system with known plaintext attack protection constructed and operative in accordance with an embodiment of the present invention.

20

DETAILED DESCRIPTION OF AN EMBODIMENT

Persons skilled in the art will appreciate that, throughout the present application, a Headend is used by way of example only, and that the present invention is not limited to a particular type of content server, but rather includes
5 any suitable device, for example, but not limited to, a video-on-demand server or a mobile phone relay station or a broadcast channel Headend.

The term “encoded” is used throughout the present specification and claims, in all of its grammatical forms, to refer to any type of data stream encoding including, for example and without limiting the scope of the definition, well
10 known types of encoding such as, but not limited to, MPEG-2 encoding, H.264 encoding, VC-1 encoding, and synthetic encodings such as Scalable Vector Graphics (SVG) and LASER (ISO/IEC 14496-20), and so forth. It is appreciated that an encoded data stream generally requires more processing and typically more time to read than a data stream which is not encoded. Any recipient of encoded
15 data, whether or not the recipient of the encoded data is the intended recipient, is, at least in potential, able to read encoded data without requiring cryptanalysis. It is appreciated that encoding may be performed in several stages and may include a number of different processes, including, but not necessarily limited to: compressing the data; transforming the data into other forms; and making the data
20 more robust (for instance replicating the data or using error correction mechanisms).

The term “compressed” is used throughout the present specification and claims, in all of its grammatical forms, to refer to any type of data stream compression. Compression is typically a part of encoding and may include image
25 compression and motion compensation. Typically, compression of data reduces the number of bits comprising the data. In that compression is a subset of encoding, the terms “encoded” and “compressed”, in all of their grammatical forms, are often used interchangeably throughout the present specification and claims.

Similarly, the terms “decoded” and “decompressed” are used throughout the present specification and claims, in all their grammatical forms, to refer to the reverse of “encoded” and “compressed” in all their grammatical forms.

The terms “scrambled” and “encrypted”, in all of their grammatical forms, are used interchangeably throughout the present specification and claims to refer to any appropriate scrambling and / or encryption methods for scrambling and / or encrypting a data stream, and / or any other appropriate method for intending to make a data stream unintelligible except to an intended recipient(s) thereof. Well known types of scrambling or encrypting include, but are not limited to DES, 3DES, CSA and AES. Similarly, the terms “descrambled” and “decrypted” are used throughout the present specification and claims, in all their grammatical forms, to refer to the reverse of “scrambled” and “encrypted” in all their grammatical forms.

Pursuant to the above definitions, the terms “encoded”; “compressed”; and the terms “scrambled” and “encrypted” are used to refer to different and exclusive types of processing. Thus, a particular data stream may be, for example:

encoded, but neither scrambled nor encrypted;
compressed, but neither scrambled nor encrypted;
scrambled or encrypted, but not encoded;
scrambled or encrypted, but not compressed;
encoded, and scrambled or encrypted; or
compressed, and scrambled or encrypted.

Likewise, the terms “decoded” and “decompressed” on the one hand, and the terms “descrambled” and “decrypted” on the other hand, are used to refer to different and exclusive types of processing.

Reference is now made to Fig. 1, which is a partly pictorial, partly block diagram view of a Headend system 10 encoding and encrypting data.

The Headend system 10 includes an encoder 12 and a multiplexer 14. The multiplexer includes an encryption processor 16.

The encoder 12 is operative to encode data 18, for example, but not limited to, audio or video data, yielding a plurality of encoded packets 20. The
5 encoding may be performed in accordance with any suitable encoding standard, for example, but not limited to, MPEG-2, MPEG-4 or VC-1.

The encoded packets 20 are typically encrypted by the encryption processor 16 based on a key or control word 22 thereby yielding a plurality of encrypted packets 24. In order to enhance security the control word 22 is typically
10 changed periodically according to a plurality of cryptoperiods.

Reference is now made to Fig. 2, which is a partly pictorial, partly block diagram view of a known plaintext attack against the Headend system 10 of Fig. 1.

In some encryption systems such as DVB CSA, every plaintext
15 packet 20 is encrypted independently so that the same plaintext packet payload on encryption (in the same cryptoperiod) yields the same ciphertext packet payload. Therefore, packets 20 having the same payload may be identified with ease and possibly subject to a plaintext attack. As an aside, even without repetition, known plaintext attacks may be mounted if the position of a known plaintext in the stream
20 is known to the attacker or the known plaintext can be otherwise identified. However, due to the complex structure of DVB CSA changing a single bit of the plaintext payload in DVB CSA generally changes the entire ciphertext. Therefore, as DVB CSA was designed to encrypt video and audio packets which are generally dynamic, ciphertext of video and audio packets are generally not subject
25 to plaintext attacks. The term DVB CSA is defined herein to any other relevant version of DVB CSA, for example, but not limited to, DVB CSA2.

However, it has been discovered that the encoder 12 may produce some encoded packets 20 where the payload of the encoded packets 20 is the same. For example, MPEG-2 encoders may produce some encoded packets 20
30 where the payload includes only zeros. It is believed that one reason for the outputting of the “zero payload” packets 20 is because the encoder 12 pre-

allocates a certain amount of packets for a frame of video, and if the encoder 12 succeeds to compress a video frame into less packets than the pre-allocated amount, the encoder 12 creates the remaining pre-allocated packets 20 with zeros. Therefore, the encoder 12 may regularly output “zero payload” packets 20 so that
5 in each cryptoperiod, the encoder 12 is outputting one or more “zero payload” packets 20.

Therefore, an attacker may identify the ciphertext of a known plaintext (in this case the “zero payload” packets 20) and mount a plaintext attack using any suitable method, for example, a time memory trade off (TMTO) or
10 rainbow table and determine the control word 22.

It should be noted that known plaintext is not only limited to “zero payload” packets 20, but will include any packets 20 which repeat with enough frequency or otherwise known to an attacker even without repetition, for example, but not limited to, packets 20 wherein the value of each byte in the payload of each
15 packet 20 is either zero or FF.

A suspected known plaintext, as used in the claims and specification, is defined herein as any plaintext which could possibly be known to an attacker due to repetition, known location and/or another method of identification to enable an attacker to mount a plaintext attack to determine the
20 cryptographic key encrypting the ciphertext.

Reference is now made to Fig. 3, which is a partly pictorial, partly block diagram view of a Headend system 28 with known plaintext attack protection constructed and operative in accordance with a first embodiment of the present invention.

25 The Headend system 28 typically includes an encoder 30, a post encoding processor 32 and a multiplexer 34. The multiplexer 34 typically includes an encryption processor 36. The post encoding processor 32 may be implemented as part of the encoder 30 or as part of the multiplexer 34 or as a separate processing unit or as part of another processor in the Headend system 28. The post
30 encoding processor 32 may even be implemented as a remote service external to

the Headend system 28 accessed via a suitable network or Internet connection, by way of example only.

The encoder 30 is typically operative to encode input data 38 yielding a plurality of data packets 40. The input data 38 encoded by the encoder
5 is typically video or audio data. Each of the data packets 40 has a header 42 and a payload 44.

By way of introduction, in order to protect against known plaintext attacks, the post encoding processor 32 is functionally disposed between the output of the encoder 30 and the input of the encryption processor 36. The post
10 encoding processor 32 identifies data packets 40 with a suspected known plaintext and modifies the identified data packets 40 so that a known plaintext attack cannot occur, as will now be described in more detail.

The post encoding processor 32 is typically operative to identify the data packets 40 having a payload with a suspected known plaintext, for example,
15 but not limited to, wherein the payload 44 of the data packets 40 only includes zeros.

The post encoding processor 32 processor is operative to compare the payload 44 of each of the data packets 40 with one or more suspected known plaintexts in order to identify the data packets 40 having the payload 44 with a
20 suspected known plaintext. Another method identifying known plaintext payloads 44 is based on looking at payload repetition and is described in more detail with reference to Fig. 6.

The post encoding processor 32 is operative to modify some or all of the identified packets 40. As described above with reference to Fig. 2, a known
25 plaintext attack is possible even if only one known plaintext exists in each cryptoperiod. A known plaintext attack is typically easier when the known plaintext occurs more than once in a cryptoperiod. Therefore, it is better to modify all the identified packets 40 and not just some of them. However, just modifying some of the data packets 40 may offer some protection against attack and may be
30 useful in some cases.

Different methods for modifying the identified data packets 40 are described with reference to Figs. 3-5. Any one of these methods may be used to modify the identified data packets 40. However, it will be appreciated that one of the methods may be used for some of the identified packets 40 while other methods may be used to modify other identified data packets 40.

One method of modifying the identified data packets 40 is now described below.

The post encoding processor 32 is operative to: remove the payload 44 of some, or all, of the identified data packets 40 so that the payload 44 of each modified packet 40 no longer exists; and add an adaptation field 52 or lengthen a pre-existing adaptation field 52 of each of the modified packets 40 to take the place of the removed payload 44. An adaptation field is an MPEG feature for conveying certain information. The content of the adaptation field is generally not encrypted. It will be appreciated by those ordinarily skilled in the art that the Headend system 28 may be implemented in non-MPEG encoding environments employing features similar to the adaptation field, so that the newly created/lengthened field(s) taking the place of the payload 44 is not encrypted.

The flags of the adaptation field 52 may be set to zero and the stuffing bytes will then be defined by MPEG-2 as all ones. Alternatively, any private data could be inserted into the stuffing bits and the transport_private_data_flag is set to 1. It will be appreciated by those ordinarily skilled in the art that there are many other options for the content of the adaptation field 52.

First, as the payload 44 of the modified packets 40 no longer exists, an attacker can no longer learn anything from the payloads 44 of the modified packets 40 to mount a known plaintext attack. Additionally, the modified packets 40 are not typically encrypted by the encryption processor 36 as the modified packets 40 do not include a payload, therefore an attacker cannot learn anything from the modified packets 40 to mount a known plaintext attack.

The encryption processor 36 is typically operative to encrypt the data packets 40 having the payload 44 yielding encrypted data packets 46 but not

to encrypt the data packets 40 not having the payload 44. The encryption processor 36 is operative to encrypt the data packets 40 in accordance with a plurality of cryptoperiods and a plurality of keys 48 such that a different key 48 is used to encrypt the data packets 40 in different cryptoperiods.

5 The above method of modifying the identified data packets 40 may be problematic in certain situations as will now be described below. The header 42 of each data packets 40 may include a continuity counter 50 added by the encoder 30. When the encoder 30 creates a packet 40 without a payload, the continuity counter 50 of that packet has the same value as the prior packet. The
10 continuity counter 50 is then incremented for the next packet with a payload. Therefore, if the payload 44 of the data packets 40 is removed and replaced with the adaptation field 52, the incorrect use of the continuity counter 50 may cause problems in a receiver-decoder where the continuity counter 50 is used to detect packet loss or used for packet indexing and possibly cause problems in the
15 multiplexer 34. Additionally, if the packet 40 after the known plaintext packet 40 includes video data then some of the final bits of the “known plaintext” packet 40 may be needed for the start of the video data of the next video packet.

 In accordance with an embodiment of the present invention, the post encoding processor 32 is operative to change the continuity counter of the
20 packets 40 so that the continuity counter 50 of each of the packets 40 without a payload has the same value as the previous packet 40 and the continuity counter 50 of the packets 40 with a payload increments sequentially so that the continuity counter 50 of each packet 40 with a payload is one count higher than the previous packet 40.

25 Although, the Headend system 28 has been described for use with an MPEG type system, it will be appreciated that Headend system 28 may be implemented for use with any suitable encoding standard, using any suitable encryption method and any suitable multiplexing system. The Headend system 28 is not limited to known plaintext where the payload only includes zeros, but may
30 be implemented for any suitable known plaintext.

The identification performed by the post encoding processor 32 may be performed online or offline. In other words, the identification may be performed in batch and the modification of the identified packets may be performed at a later time once the identification process for a particular content
5 item has been completed. Alternatively, the identification and modification may be performed at the same time in an online fashion so that as one packet is being screened for known plaintext another packet is modified.

Reference is now made to Fig. 4, which is a partly pictorial, partly block diagram view the Headend system 28 of Fig. 3 operating in accordance with
10 an alternative mode of operation.

Another method of modifying the identified packets 40 is now described below.

The post encoding processor 32 is operative to modify the payload 44 of some, or all, of the identified packets 40 so that the payload 44 of
15 each modified packet 40 is no longer a suspected known plaintext.

As each modified data packet 40 still includes the payload 44, the encryption processor 36 is operative to encrypt the data packets 40, including the data packets 40 with the modified payload 44, yielding encrypted data packets 46.

The post encoding processor 32 may be operative to replace the
20 payload 44 of some, or all, of the identified data packets 40 with random or pseudo-random data or other broadcast data, for example, but not limited to, an entitlement management message (EMM), an entitlement control message (ECM), electronic program guide data, event information table (EIT) data, non-zero audio data, non-zero video data and/or metadata for the audio data or the video data. The
25 non-zero audio and video data may relate to content pushed to the storage devices of receiver-decoder devices (for example, a personal video recorder (PVR)) by a broadcaster or content provider or service provider.

If the payload 44 is replaced by random or pseudo-random data, the data needs to be carefully crafted in order not to confuse a receiver-decoder device
30 which will be a recipient of the modified data packets 40.

One advantage of the modification method described with reference to Fig. 4 is that if the payload 44 is maintained and the packet ID (PID) remains unchanged (for example, when the data is replaced by random or pseudo-random data), then the continuity counter 50 is also maintained.

5 An additional advantage is that the modified payload may be utilized for carrying useful broadcast data thereby utilizing what would have been wasted bandwidth. However, when the modified payload 44 includes useful broadcast data, the PID of the modified packet 40 is often modified to reflect the change in the type of payload 44. Therefore, the continuity counter(s) of the data
10 packets 40 may need to be modified so that for each PID which has a continuity counter 50, the continuity counter 50 in the header 42 of the data packets 40 with the payload 44 will be continuous without gaps. Therefore, the post encoding processor 32 is operative to change the continuity counter of some, or all, of the packets 40 to compensate for the modification of the identified packets 40.

15 Reference is now made to Fig. 5, which is a partly pictorial, partly block diagram view of the Headend system 28 of Fig. 3 in accordance with another alternative mode of operation.

Another method of modifying the identified packets 40 is now described below.

20 The post encoding processor 32 is operative to: reduce the length of the payload 44 of some, or all, of the identified packets 40 to less than a "certain" length; and add an adaptation field 54 to each modified packet 40 or lengthen a pre-existing adaptation field 54 of each modified packet 40 to compensate for the shortened payload 44. As described above with reference to Fig. 3, the content of
25 the adaptation field is generally not encrypted. It will be appreciated by those ordinarily skilled in the art that the Headend system 28 may be implemented in non-MPEG encoding environments employing features similar to the adaptation field, so that the newly created/lengthened field(s) filling in for the shortened payload 44 is not encrypted.

30 In accordance with DVB CSA, packets with payloads of less than 8 bytes are not encrypted. Therefore, by reducing the payload 44 to between 2 and 7

bytes, the modified packets 40 are not encrypted and therefore an attacker cannot mount a plaintext attack based on the modified packets 40. Therefore, for a DVB CSA encryption system, the “certain” length is equal to eight bytes. It will be appreciated by those ordinarily skilled in the art that for other encryption systems the “certain” length may be different or not a relevant factor.

The formatting of the adaptation field 54 was discussed in more detail above with reference to Fig. 3.

One advantage of the modification method described with reference to Fig. 5 is that as the payload 44 is maintained (although reduced in length), the continuity counter 50 is also maintained.

Additionally, if the packet 40 after the known plaintext packet 40 includes video data then some of the “final bits” of the “known plaintext” packet 40 may be needed for the start of the video data of the next video packet and in the scenario described with reference to Fig. 5 the “final bit” data is maintained in the reduced payload 44.

The encryption processor 36 is operative to encrypt the data packets 44 having the payload 44 with a length greater than or equal to the “certain” length yielding the encrypted data packets 46 but not encrypt the data packets 40 having the payload 44 with a length less than the “certain” length.

Reference is now made to Fig. 6, which is a partly pictorial, partly block diagram view of an encoding and post processing system 56 with known plaintext attack protection constructed and operative in accordance with an embodiment of the present invention.

The system 56 includes an encoder 58 and a post encoding processor 60.

The encoder 58 is operative to encode input data 62 yielding a plurality of data packets 64. Each packet 64 has a header 66 and a payload 68.

The post encoding processor 60 is operative to: search the payload 68 of each of the packets 64 in order to find packets 64 with matching payloads 68 (block 70); select packets 64 from the matching payload packets 64

where the same payload 68 repeats in accordance with one or more frequency requirements (block 72); and assign the selected packets 64 as suspected known plaintext packets 64 (block 74).

As only scrambled packets are useful for a hacker, the search step
5 listed above (block 70) only needs to search packets 64 which will be encrypted. In many MPEG DVB systems, only packets with an audio or video packet ID (PID) are scrambled.

Broadly speaking, the frequency requirements are set to find packets which repeat with such frequency so that the packets are useful for attackers to
10 mount a known plaintext attack. An example of a frequency requirement is as follows.

When the data packets 64 will be encrypted (by the system 56 or another system) a plurality of cryptoperiods and a plurality of keys may be used such that a different key is used to encrypt the data packets in each different
15 cryptoperiod. In such as case, the frequency requirements may include requiring that there could potentially be matching payload packets 64 having the same payload 68 at least once (or alternatively at least twice) in each cryptoperiod.

The system 56 may be a stand alone system or as part of a Headend system including packet modification, encryption and multiplexing.

20 In practice, some or all of these functions may be combined in a single physical component or, alternatively, implemented using multiple physical components. These physical components may comprise hard-wired or programmable devices, or a combination of the two. In some embodiments, at least some of the functions of the processing circuitry may be carried out by a
25 programmable processor under the control of suitable software.

It is appreciated that software components of the present invention may, if desired, be implemented in ROM (read only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques. It is further appreciated that the software components
30 may be instantiated, for example, as a computer program product; on a tangible medium; or as a signal interpretable by an appropriate computer.

It will be appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single
5 embodiment may also be provided separately or in any suitable sub-combination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined by the appended claims and equivalents thereof.

10

What is claimed is:

CLAIMS

1. A system comprising:
an encoder to encode input data yielding a plurality of data packets,
5 each of the packets having a header and a payload;
a post encoding processor to:
identify ones of the data packets having a payload with a
suspected known plaintext; and
modify at least some of the identified packets; and
10 an encryption processor to encrypt at least some of the data packets
yielding encrypted data packets.
2. The system according to claim 1, wherein:
the post encoding processor is operative to modify the payload of
the at least some identified packets so that the payload of each of the at least some
15 identified packets is no longer a suspected known plaintext; and
the encryption processor is operative to encrypt the data packets
yielding the encrypted data packets.
3. The system according to claim 2, wherein the post encoding
processor is operative to replace at least some of the data of the payload of each of
20 the at least some identified packets with random or pseudo-random data.
4. The system according to claim 2, wherein the post encoding
processor is operative to replace at least some of the data of the payload of each of
the at least some identified packets with other broadcast data.
5. The system according to claim 4, wherein the other broadcast data is
25 selected from at least one of: an entitlement management message (EMM), an

entitlement control message (ECM), electronic program guide data, event information table (EIT) data, non-zero audio data, non-zero video data and metadata for the audio data or the video data.

6. The system according to claim 1, wherein:
5 the post encoding processor is operative to:
remove the payload of the at least some identified packets so
that the payload of each of the at least some identified packets no longer exists;
and
for each one of the at least some identified packets, add an
10 adaptation field to the one identified packet or lengthen a pre-existing adaptation
field of the one identified packet; and
the encryption processor is operative to encrypt the data packets
having the payload yielding the encrypted data packets but not to encrypt the data
packets without the payload.

- 15 7. The system according to claim 1, wherein:
the post encoding processor is operative to:
reduce the length of the payload of each of the at least some
identified packets to less than a certain length; and
add an adaptation field to each of the at least some identified
20 packets or lengthen a pre-existing adaptation field of each of the at least some
identified packets; and
the encryption processor is operative to encrypt the data packets
having the payload with a length greater than or equal to the certain length
yielding the encrypted data packets but not encrypt the data packets having the
25 payload with a length less than the certain length.

8. The system according to claim 7, wherein the certain length is equal
to eight bytes.

9. The system according to any of claims 1-8, wherein each of the bytes of the payload with the known plaintext is only selected from a value of zero and FF.
10. The system according to any of claims 1-9, wherein the input data
5 encoded by the encoder is video data.
11. The system according to any of claims 1-10, wherein the post encoding processor is operative to compare the payload of each of the data packets with at least one suspected known plaintext in order to identify the data packets having the payload with a suspected known plaintext.
- 10 12. The system according to any of claims 1-10, wherein the post encoding processor is operative to:
- search the payload of each of the packets in order to find packets with matching payloads;
 - select packets from the matching payload packets where the same
15 payload repeats in accordance with at least one frequency requirement; and
 - assign the selected packets as suspected known plaintext packets.
13. The system according to claim 12, wherein:
- the encryption processor is operative to encrypt the at least some data packets in accordance with a plurality of cryptoperiods and a plurality of keys
20 such that a different one of the keys is used to encrypt the data packets in a different one of the cryptoperiods; and
 - the at least one frequency requirement is that there could potentially be matching payload packets having the same payload at least once in each of the cryptoperiods.
- 25 14. The system according to any of claims 1-13, wherein:
- the encoder is operative to add a continuity counter to the header of each of the packets; and

the post encoding processor is operative to change the continuity counter of at least some of the packets to compensate for the modification of the at least some identified packets.

15. A method comprising:
- 5 encoding input data yielding a plurality of data packets, each of the packets having a header and a payload;
- identifying ones of the data packets having a payload with a suspected known plaintext;
- modifying at least some of the identified packets; and
- 10 encrypting at least some of the data packets yielding encrypted data packets.

16. A system comprising:
- an encoder to encode input data yielding a plurality of data packets, each of the packets having a header and a payload;
- 15 a post encoding processor to:
- search the payload of each of the packets in order to find packets with matching payloads;
- select packets from the matching payload packets where the same payload repeats in accordance with at least one frequency requirement; and
- 20 assign the selected packets as suspected known plaintext packets.

17. The system according to claim 16, wherein:
- at least some of the data packets will be encrypted in accordance with a plurality of cryptoperiods and a plurality of keys such that a different one of
- 25 the keys is used to encrypt the data packets in a different one of the cryptoperiods; and
- the at least one frequency requirement is that there could potentially be matching payload packets having the same payload at least once in each of the cryptoperiods.

18. A method comprising:
- encoding input data yielding a plurality of data packets, each of the packets having a header and a payload;
 - searching the payload of each of the packets in order to find packets
 - 5 with matching payloads;
 - selecting packets from the matching payload packets where the same payload repeats in accordance with at least one frequency requirement; and
 - assigning the selected packets as suspected known plaintext packets.

10

Fig. 1

1/6

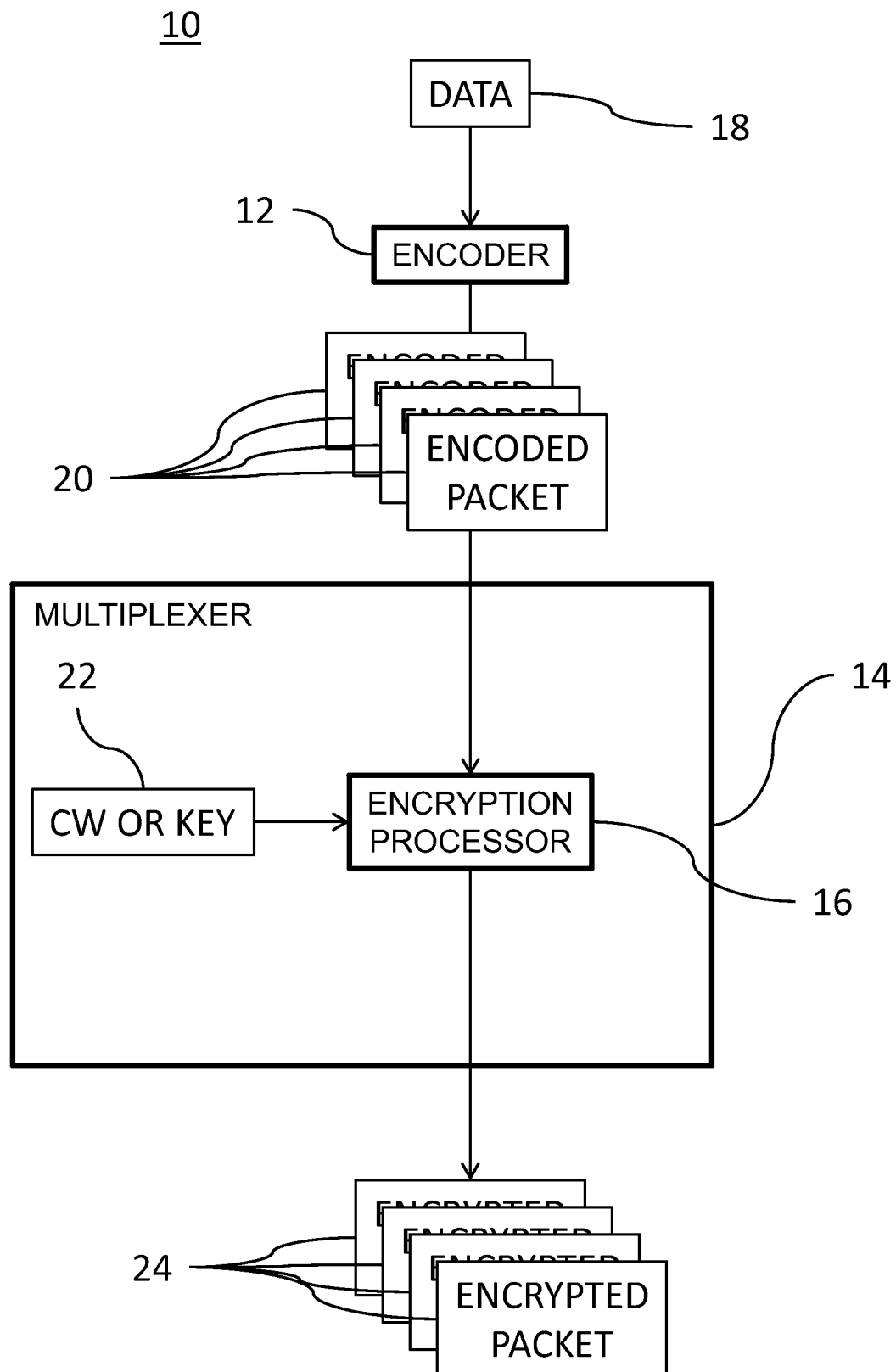


Fig. 2

2/6

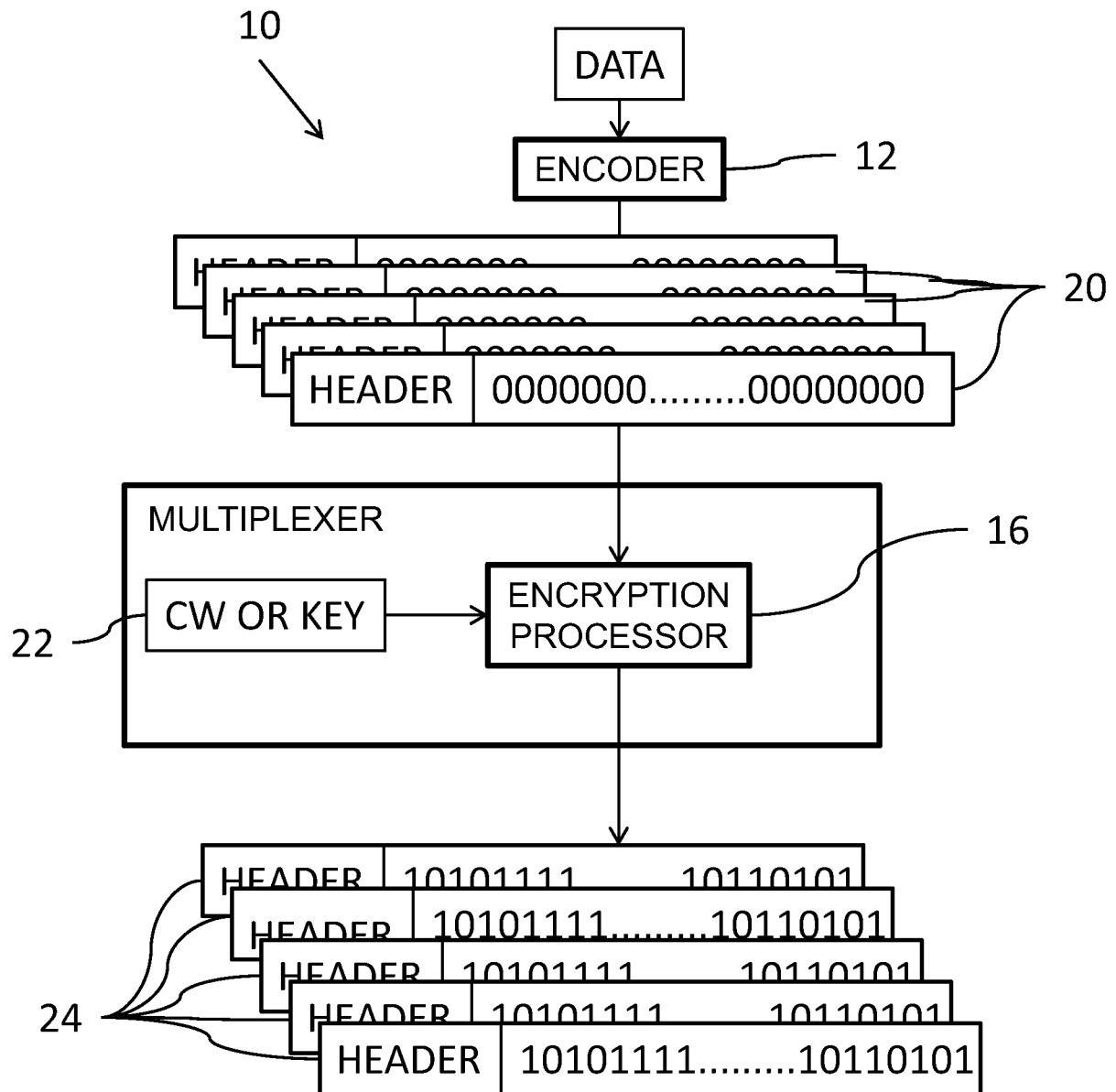


Fig. 3

3/6

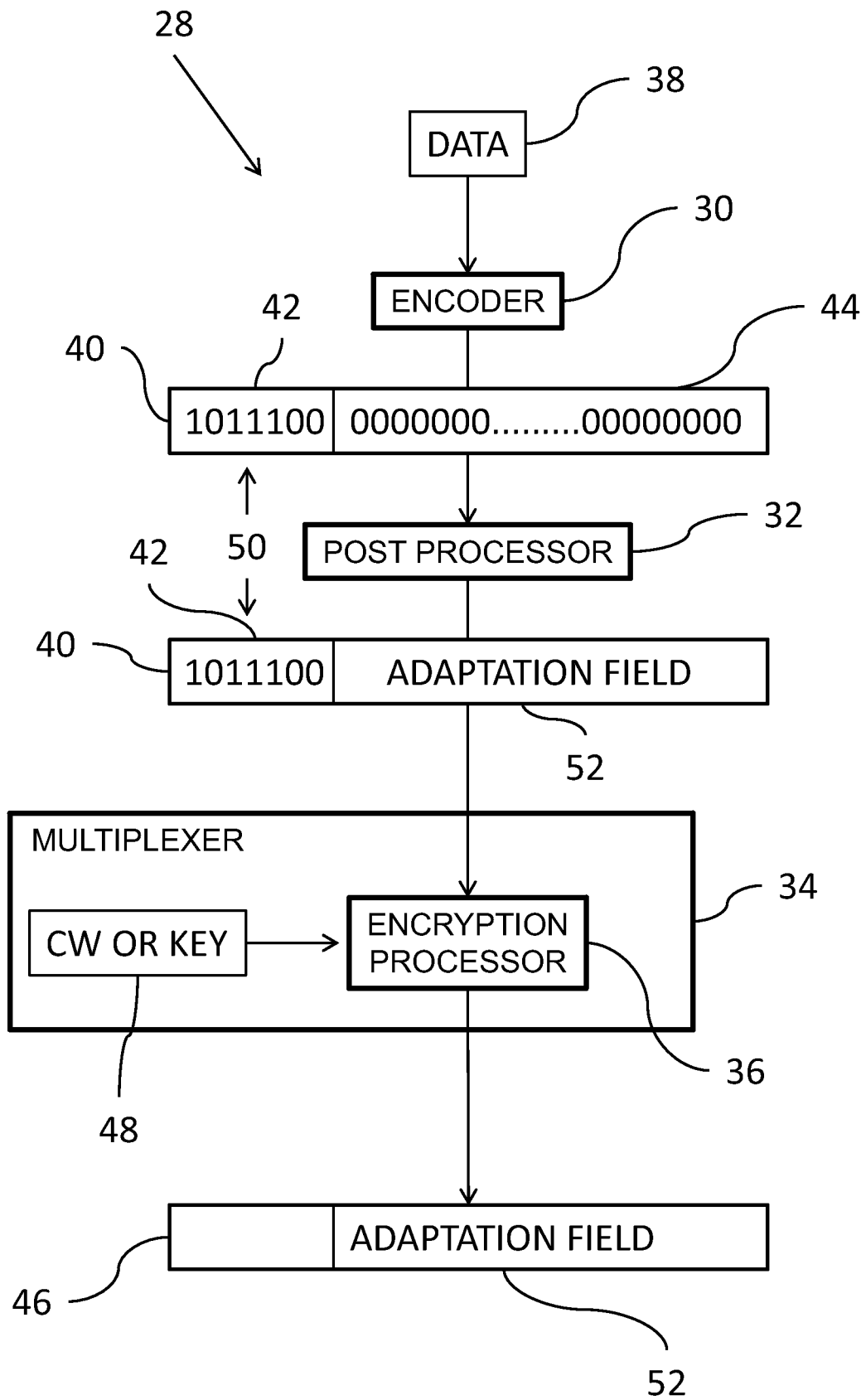


Fig. 4

4/6

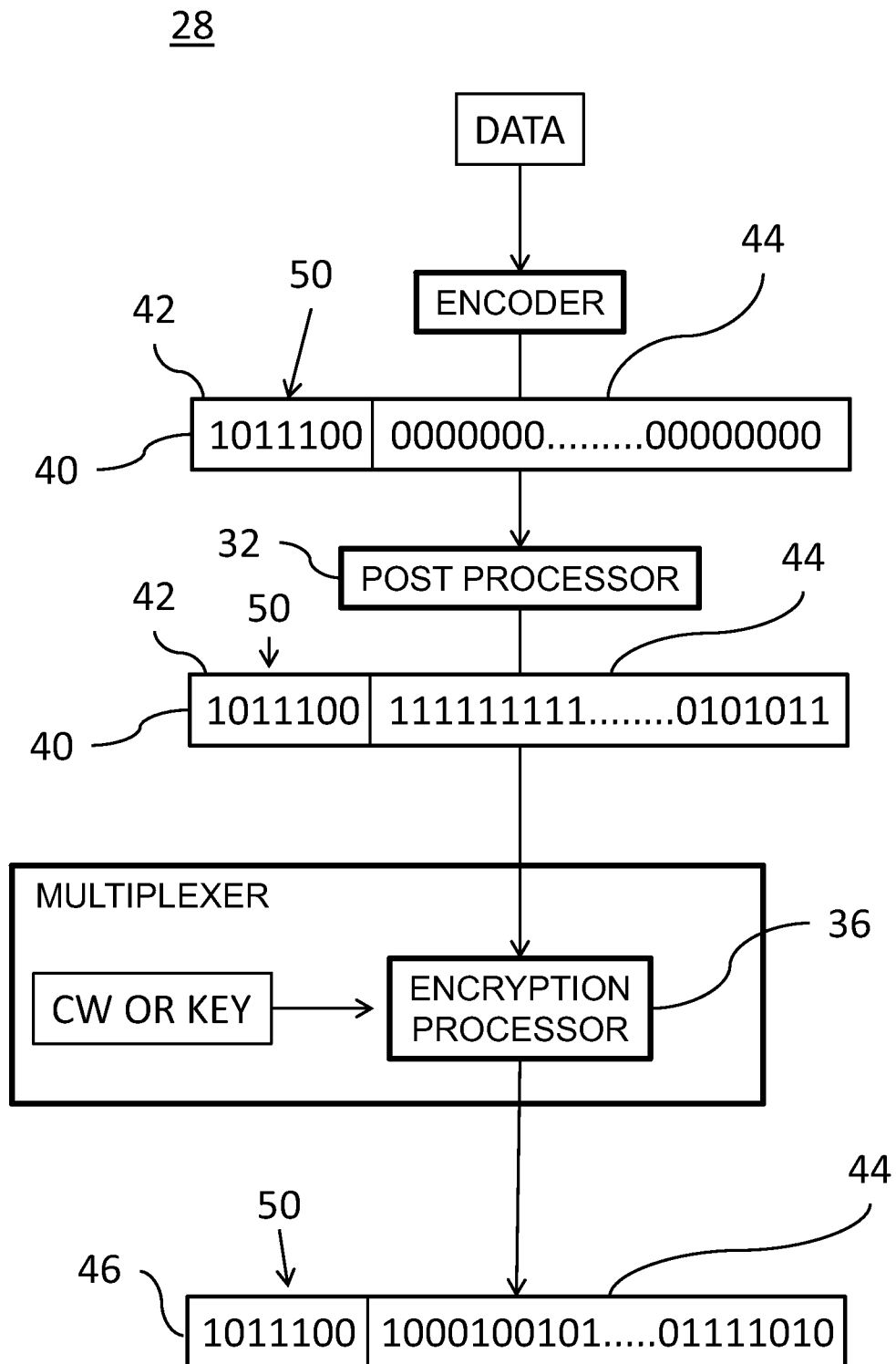


Fig. 5

5/6

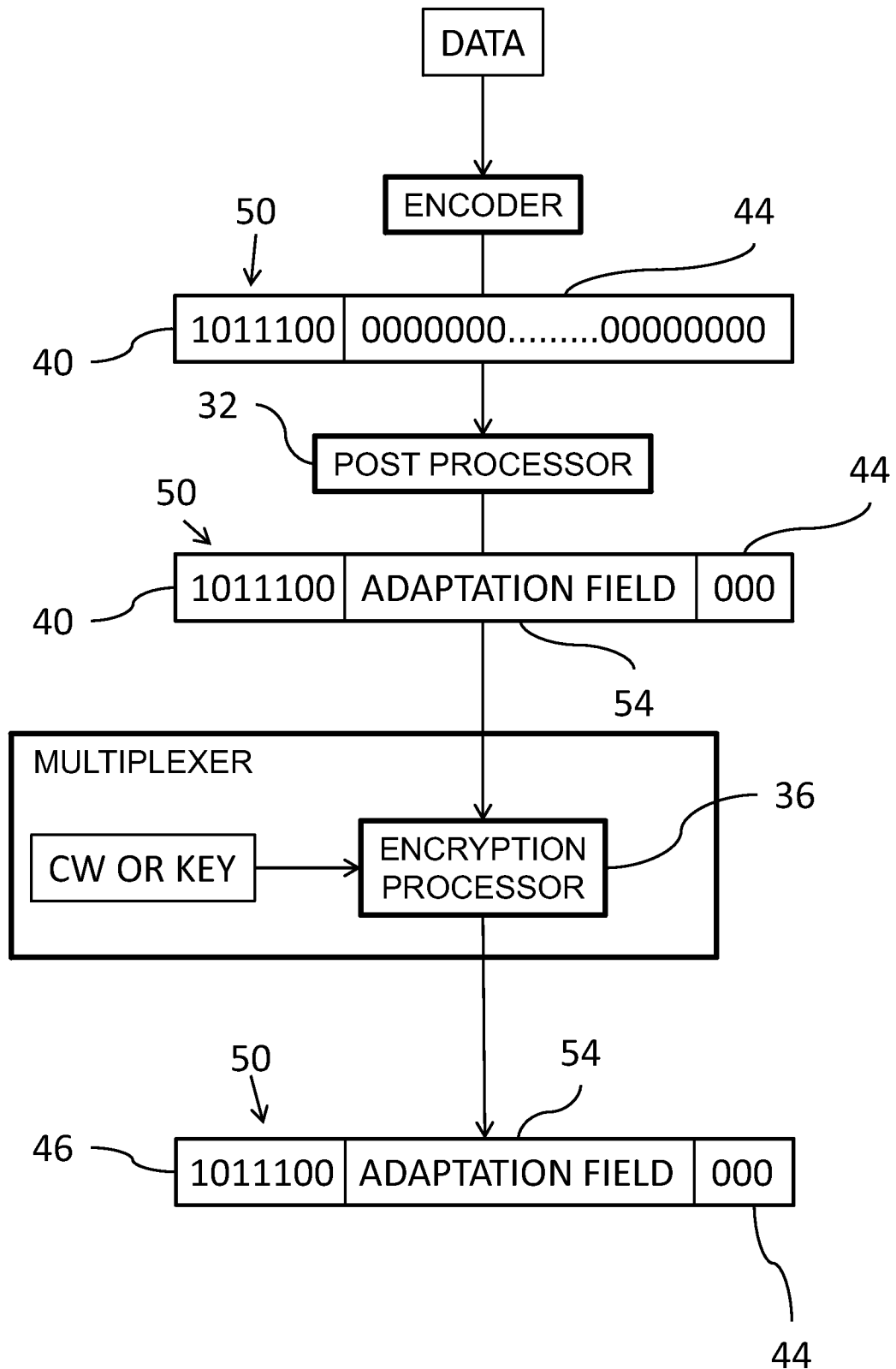
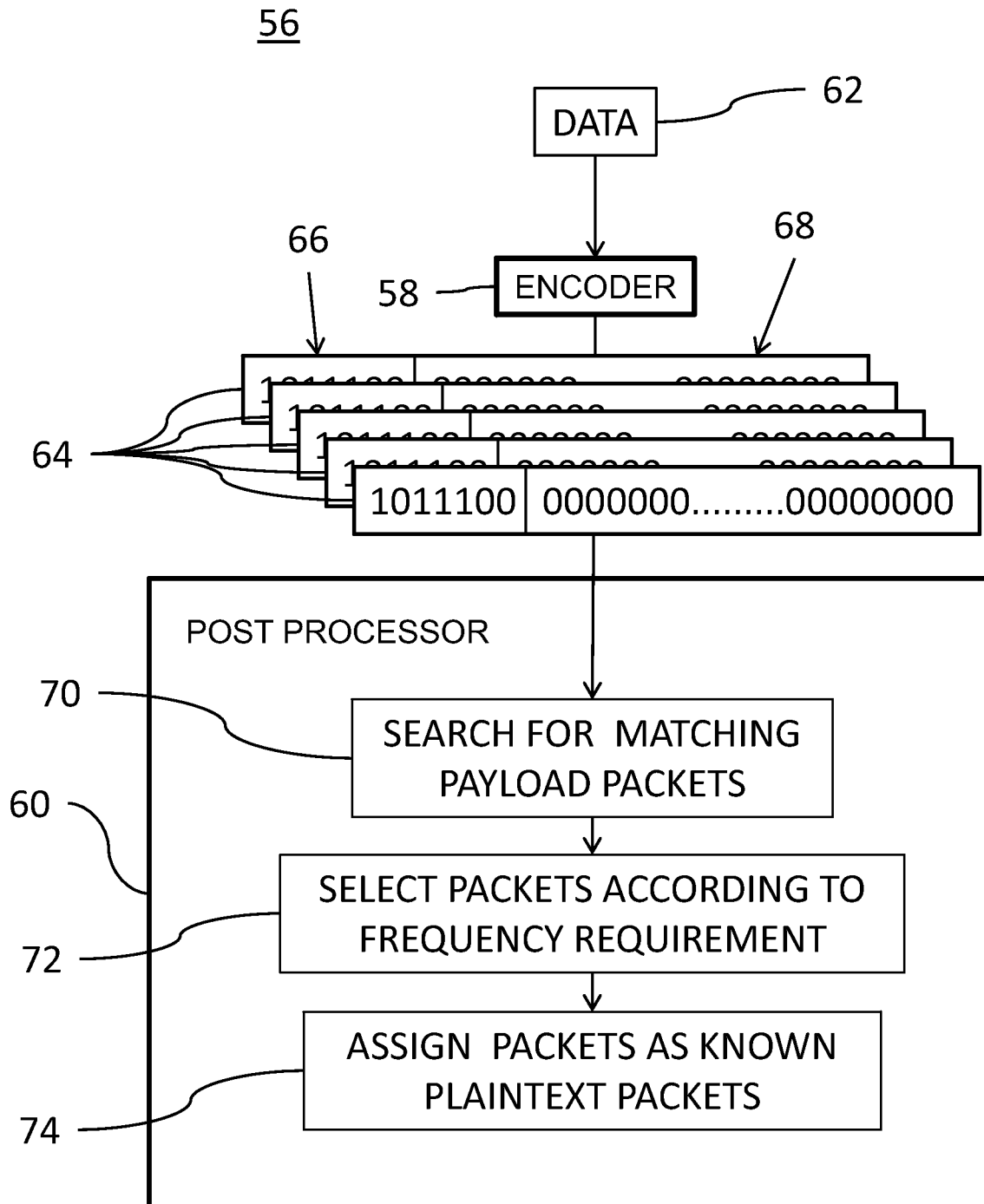
28

Fig. 6

6/6



INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/057428

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 G06F21/55
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/135486 A1 (SCHNEIDER JAMES P [US]) 3 June 2010 (2010-06-03) abstract paragraphs [0004], [0026] - [0042], [0052] - [0070] figures 1-2B,4,6	1-18
X	EP 2 148 462 A1 (UNIV CORK [IE]) 27 January 2010 (2010-01-27) abstract paragraphs [0020] - [0029], [0060] - [0129] figures 1-11 ----- -/-	1-18

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 April 2013

Date of mailing of the international search report

25/04/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Mariggis, Athanasios

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2012/057428

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ERIK TEWS ET AL: "Breaking DVB-CSA", 20 July 2011 (2011-07-20), RESEARCH IN CRYPTOLOGY, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 45 - 61, XP047020093, ISBN: 978-3-642-34158-8 cited in the application the whole document -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2012/057428

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2010135486	A1	03-06-2010	NONE	

EP 2148462	A1	27-01-2010	NONE	
