

IN THE UNITED STATES RECEIVING OFFICE

*Application
for
International Patent Application
in accordance with the terms of the
Patent Cooperation Treaty*

**Method for Secure Delivery
of Digital Content**

Applicant: SkyVault Secure Digital Distribution, Inc.
Inventor: David K. Probst

METHOD AND APPARATUS FOR SECURE DELIVERY OF DATA

The present invention pertains to methods and apparatus for ensuring the security of data such as digital content. More particularly, one preferred embodiment of the invention provides copy protection for digital content that is displayed or recreated on a player or terminal of an end user.

5

Content providers are increasingly storing and distributing their intellectual property works (that is, the content) in digitised form and are justifiably concerned about the possibility that this content may be misappropriated. Conventional security methods encrypt the digital content, transmit the content to the user, and trust the user's player or terminal to decrypt it in a secure fashion. Many of these conventional security methods may easily be broken because they utilise weak proprietary or open source cryptographic algorithms and protocols that are easily broken by hackers of moderate skill who promptly publish their results, nullifying the original security system.

15 At the present time, none of the security systems which are available in the commercial market can provide reliable copy protection. The development of such a system would constitute a major technological advance, and would satisfy long felt needs and aspirations in the both the content producing (entertainment, games, software, etc.) and telecommunications (telephone, cable, satellite networks, etc.) industries.

20

The present invention seeks to provide an improved method and apparatus for the secure delivery of data, particularly digital data.

25 According to an aspect of the present invention, there is provided a method of securing data transmitted to a user device from a content provider as specified in claim 1.

According to another aspect of the present invention, there is provided a system for transmitting data securely to a user device from a content provider as specified in claim 13.

30 The preferred embodiment supplies a means of copy protection for digital content. In one embodiment of the invention, all responsibility for copy protection is removed

from the user's player or terminal. All the security features are removed from the player, and placed in a secure "box". The box incorporates security protocols that use strong cryptographic algorithms as primitives to seek to ensure that the security furnished by the module cannot be broken.

5

In one embodiment, a delivery source or station sends a time-bounded computational ability to display the content separately from the digital content and then self-destructs. The division of labour between station and box means that unusually strong encryption algorithms may be employed, while keeping the cost of manufacture of the box low since they require relatively little processing power. When the box is purchased, a registration process enters a security protocol.

The preferred embodiments offer a distributed end-to-end system/security architecture that is completely independent of the communications medium which is employed. They may be utilised to secure or protect any digital content, including high value files that contain movies or music which are transported over a network, or which are stored on a physical medium such as a DVD or CD.

Embodiments of the present invention are described below, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of one embodiment of system;

Figure 2 is a schematic diagram of one embodiment of box;

25

Figure 3 is a flow chart of an embodiment of encryption processing routine carried out at a station; and

Figure 4 is a flow chart of an embodiment of recovery routine.

30

One embodiment comprises a method for copy protection for the owner of digital content that is displayed on a user's player or terminal. The responsibility for copy protection is removed from the player, and is placed inside an appliance or terminal in a secure "box."

5

In a preferred embodiment of the invention, cryptographic primitives (encryption algorithms, message-authentication codes, hash functions, random-number generators, and so on) are used in a novel security protocol together with a novel key exchange protocol. The system may be utilised to protect a first-run movie that has been digitised in accordance with one of the current or forthcoming standards (such as MPEG). Content receivers or users first register their boxes. This registration information is stored in a secure database. When a subscriber registers, he/she then receives a box (interface to the player) that has been initialised to contain a number of tamper-proof secrets that are shared between the station and that particular box. The station stores an encrypted version of the digital content. This encrypted version ultimately arrives at some unprotected storage medium local to the player. Upon demand, the station delivers to the box the use-once computational ability to decrypt the content and display it on the player or terminal.

The box is configured for a computational workload that allows it to be manufactured relatively cheaply. The station is configured for a computational workload that allows it to keep pace with what might be one million simultaneous requests for service from one million boxes. In one embodiment, the box is a modest-sized information appliance, while a station comprises a cluster of workstations (or equivalent) as the number of boxes per station grows. Initial encryption of the digital content and security-domain initialisation of station and box both count as pre-computation in the preferred embodiment.

In the preferred embodiment, the encrypted content or ciphertext is stored on a removable or fixed storage medium within the user's player. The subscriber then requests the content provider to supply a "key" which enables the box to play the content. This

30

request may require a payment from the subscriber to the content provider. Once the content provider is paid, or approval to decrypt the content stored in the user's box is granted, the station supplies the transient computational ability to display the content once. The word "transient" is used here because the computational ability self-destructs as it is used. The subscriber may issue as many requests for use-once computational ability to display this movie as desired; this resembles "pay per view" with higher-value digital content. The embodiment may employ multiple time sensitive keys which vanish as soon as they are used.

10 The described embodiments may be utilised to secure or protect any digital content, including high value files that contain movies or music which are transported over a network or which are stored on a physical medium such as a DVD or CD.

One embodiment of the invention includes:

- 15 a) encrypting digital content;
- b) establishing a priori shared secrets between a station and a box by tamper-proof burning of secret information into boxes prior to their registration;
- c) creating a security protocol to deliver the transient computational ability to a given box to display the encrypted digital content precisely once (this ability self-
- 20 destructs as it is used); and
- d) designing the box system architecture, with particular attention paid to physical-security issues (the box's physical-security perimeter is preferably implemented by hardware means within the box).

25 Referring to Figure 3, there is shown a simplified embodiment of encryption routine carried out by the content provider for encrypting movies or other large data files for transmission of that data to a user box.

 At step 100, the content provider obtains the digital content D relating to the

30 particular file (such as movie file) requested by a user. At step 102, the file is divided into

n blocks D_j , preferably of fixed length. At step a total of n encryption keys are generated or obtained, these preferably being 256-bit keys produced by sampling noise to produce random keys. At steps 106 to 110 the routine passes through a loop to encrypt each block D_j with its appropriate key K_j by the employed encryption algorithm until all the blocks have been encrypted. Finally, at step 112, the provider outputs the encrypted blocks C_j and the keys K_j for all the blocks.

Referring now to Figure 4, the recovery routine carried out by the user's box is shown. At step 120 it receives the encrypted blocks C_j and keys K_j from the content provider, as long as the box is registered and has passed a first stage authentication test, of which examples are described below. At steps 124 to 128, the routine loops to decrypt the individual encrypted blocks C_j and to destroy each key K_j once it has been used, until all the blocks have been decrypted. At step 130, the system reassembles the individual blocks D_j into their original sequence and thereby to recover the digital content. Of course, if the blocks D_j have been sent in sequential order, then the reassembly step is straightforward. However, it is envisaged that a content provider may wish to change the order of the blocks for added security purposes.

Encryption

Before the subscriber can obtain content, such as a copy of an encrypted digital film, it must first have been encrypted. This encryption must offer extremely high-assurance confidentiality and be susceptible of decryption by equipment used by the subscriber. In one embodiment of the invention, an appropriate strong encryption algorithm is selected. For encryption of large files containing high-value digital content, a choice can be made among various methods, including symmetric-key, asymmetric-key and public-key cryptography. The throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best-known symmetric-key schemes. All operational systems use a hybrid approach that utilise both kinds of cryptography. Specifically, public-key schemes are used only for

cryptographic-key exchange, while the more efficient private-key schemes are used for actual encryption and decryption of digital content. In one embodiment of the invention, no cryptographic keys are ever made public in themselves; at most, some of them are published in a secure fashion within an individual security group. Symmetric-key methods
5 can be quite strong.

In one embodiment of the invention, the symbol “M” is used to represent a file containing a first-run movie that has been digitised according to some MPEG standard. In this particular instance, the MPEG standard also defines the decryption throughput that
10 must be achieved by the box in order that the decrypted signal may be injected into the subscriber’s player or terminal at the expected rate. (This example assumes on-the-fly decryption).

File M is divided into ‘s’ fixed-size segments, where ‘s’ is chosen by the security
15 architect. Segments are portions of a file, such as a movie. By increasing the value of ‘s’, the amount of plaintext that is encrypted can be limited by any one cryptographic key. The trade-off here is between unusually high degrees of assurance and the number of keys that must be exchanged between station and box during one key-exchange protocol. The preferred embodiments have been designed with a number of parameters so that security
20 may be increased. In general, when the level of security is increased, the performance decreases. The majority of the key-exchange work is borne by the station and is, therefore, limited only by computing power of the station.

At this point in the process, file M is a sequence of plaintext segments $\langle b_j \rangle$, $1 \leq j \leq s$. Each film segment b_j is encrypted using the Rijndael symmetric-key encryption
25 algorithm, which is the new Federal Advanced Encryption Standard (AES). Rijndael is superior to the unclassified symmetric-key algorithms it replaces in both security and performance. In one embodiment, both the block length and the key length are chosen to be
30 256 bits.

Since Rijndael is a block cipher and since it is unlikely that the length of a film segment b_j is less than or equal to 256 bits, in the case of films Rijndael is combined with an appropriate cipher-block chaining strategy such as Cipher Block Chaining (CBC). Several choices are available. A different 256-bit Rijndael key k_j is used to encrypt each film segment b_j , $1 \leq j \leq s$. The ciphertext corresponding to b_j is denoted c_j . The division into segments increases the strength of the encryption, by encrypting less plaintext with a given key, and also provides great flexibility in the decoding strategy.

No special care is required in selecting Rijndael keys. In one embodiment of the invention, keys are selected using a method that prevents a hacker from breaking the security of the system. A random-number generator or other mechanism may be employed, as long as the keys are generally unpredictable and irreproducible. In one embodiment, the 256-bit keys are genuinely random numbers produced by physical processes such as electrically noisy diodes. Genuinely random numbers are used as Rijndael keys, not to make Rijndael run better nor to prevent a hacker from breaking the security of the system, but, rather, to open up entirely new key-exchange and/or key-determination possibilities.

After encryption, the encrypted-film file $M' = \langle c_j \rangle$, $1 \leq j \leq s$, and the film-segment-key file $K = \langle k_j \rangle$, $1 \leq j \leq s$. Both encrypted-film file M' and film-segment-key file K are stored securely in the station. The plaintext file M is no longer required.

Registration & Initialisation

25

The second component concerns the initialisation of both station A and box B where there is one station A and many boxes B. Some station initialisation is done once for all boxes in the security domain and some is done on a per-box basis. Box initialisation becomes “valid” as soon as the box has been registered with the security domain.

30

1) A box-independent public-key cryptosystem is constructed for station A based on the RSA cryptosystem, but using quasi-public keys. The symbols 'p' and 'q' are employed to denote two large distinct primes. The symbol $n = p * q$. The set of plaintexts and the set of ciphertexts are both equal to the finite ring Z_n . Any message too long to belong to Z_n is dealt with by Cipher Block Chaining (CBC). Two exponents 'e' and 'd' are constructed such that exponentiation by one exponent modulo n is the inverse of exponentiation by the other exponent modulo n. One exponent, 'pubA', chosen small, is burned into each box registered with this station, along with the modulus In'. The other exponent, 'priA', which may be large, is a secret of station A. The key 'pubA' is a quasi-public key that is burned into each box B registered with A in a tamper-proof way so that 'pubA' is not recoverable from box B. The same holds true for modulus In'.

Any box B will raise numbers to the power 'pubA' modulo n to encrypt messages intended for station A and to verify digital signatures generated by station A. This is sufficient for a rapid authentication protocol that authenticates a given box B to station A provided that each box B is given a large, (for example, 256-bit) genuinely random string 'idB', which is a shared secret between A and B, that is a unique identifier for a given box B among all boxes registered with that station.

2) A box-independent large cyclic group is then constructed, in which the discrete-logarithm problem is intractable for station A. This can be done either with standard number theory or elliptic-curve techniques. One method that may be employed is to choose a large prime 'p', and then to use the multiplicative group of integers modulo p, i.e., Z^*_p , as the cyclic group. Since 'p' is a prime number, there will be many primitive elements 'x' such that raising 'x' to successive powers will generate all the elements of the cyclic group. A primitive element modulo p has the same order as the cyclic group Z^*_p , viz., $p - 1$.

This additional machinery, on top of station A's long-lasting public-key

cryptosystem, is used in the key-exchange protocol to generate session keys for encrypting the file-segment keys k_j , $1 \leq j \leq s$.

As an example, an appropriate prime 'p' and generator 'alpha' of Z^*_p ($2 \leq \text{alpha} \leq p - 2$) is selected. Quasi-ElGamal key agreement may be achieved between station A and each one of one million boxes B as follows. For a given box B, A would normally need to reliably know the public key (p, alpha, alpha^b) of B. In this example, station A has a cyclic group whose order is at least one million. Station A randomly and uniformly picks a distinct exponent 'b' $1 \leq b \leq p - 2$, for each of the one million boxes it registers. Station A secretly computes and stores alpha^b , for each box. As part of the registration process, exponent 'b' and prime 'p' are burned into the given box B (with a different 'b' for each distinct box B). When station A wishes to share a session key with a given box B, it randomly and uniformly picks an integer 'x' from the same range, and computes and transmits alpha^x , called "elementA", to box B. Station A computes $(\text{alpha}^b)^x$ modulo p as the shared secret key, while box B computes elementA^b modulo p as the key, where, by construction, the keys are the same.

Considering just the first two components, after registration, a given box B securely stores:

- 1) the small integer 'pubA', which is station A's quasi-public key;
- 2) the RSA modulus 'In';
- 3) the 256-bit quantity 'idB' that uniquely identifies the given box B;
- 4) the 20-bit quantity 'bB', which probably should not be a small integer even though the adversary has no knowledge of prime 'p'; and
- 5) the prime 'p' that is the modulus for the cyclic group Z^*_p .

Box System Architecture

In one embodiment of the invention, box B comprises two distinct modules with an extremely narrow interface. The first module is a communications module, which may

comprise a communications processor, a simplified file-transfer protocol and a local disk. As a simpler alternative, the communications module may comprise a slot into which an encrypted DVD can be inserted along with a DVD reader. The second module is a crypto module that is responsible for the key-exchange protocol and for the decryption of the encrypted digital content. The interface between the two modules is a one-way communications channel which enables the communications module to transmit the encrypted bitstream to the crypto module.

The Physical Security of the Player

10

In one embodiment of the invention, the crypto module, which includes the key-exchange module and the decryption module, is provided with exceptional physical security. The crypto module is designed to be tamper-proof in a fail-safe way. Faraday cages may be used to eliminate leakage of van Eck radiation. Volatile storage, together with “erase on tamper” deletes all keying information upon tampering with extremely high assurance. Finally, all microelectronics and wires are coated with a super glue or a potting compound which destroys the underlying circuitry if they are removed or disturbed.

The tap-proof line that runs out of the decryption module is also protected. Various anti-wiretapping strategies, including the use of piezoelectric materials, are preferably employed to signal the crypto module to “wipe clean”.

In one embodiment of the invention, the key-exchange module can deliver the file-segment keys k_j to the decryption module as plaintext. An alternative method employs the delivery of the Rijndael-encrypted k_j , along with their keys kk_j . The decryption module would then perform successive Rijndael decryptions to recover first the k_j and, then, the digital content.

Some of the properties of the box which are utilised in one embodiment of the invention are summarised below:

1) the communications module employs any communications medium to obtain the encrypted film: over the Internet, captured from a direct satellite broadcast, read in from a CD-ROM, and so on. The encrypted file is stored on disk or some storage medium nearby;

5 2) the crypto module has the following features:

a) 'idB' and 'pubA' stored in box B allow cheap secure authentication of B to A;

b) 'bB' stored in box B allows computation of the session key 'S' used to encrypt/decrypt the 's' film-segment keys k_j $1 \leq j \leq s$. The computation by box B is $S = \text{elementA}^{bB} \text{ modulo } p$, where 'elementA' is transmitted in plaintext from A to B, and
10 'bB' and 'p' are secrets of box B.

The station delivers 's' 256-bit keys k_j to the requesting box, which is $256 * s$ bits altogether. But each of the k_j keys was chosen as a genuinely random number using some random physical process. It follows that the concatenation of all the keys k_j in ascending
15 order is a plaintext of length $256 * s$ bits with no redundancy whatsoever, unlike what would be expected if the plaintext were a human-comprehensible message expressed in a natural language such as English.

As their name indicates, one-time pads are never supposed to be used more than
20 once because that would allow an adversary to exploit the redundancy of the underlying plaintext. Transmission of perfectly random plaintext allows the system to realise efficiencies that are forbidden to ordinary plaintext.

Station A and a given box B have a fixed shared secret (the 256-bit quantity that
25 uniquely identifies box B), and a variable shared secret which changes with every invocation of the key-exchange protocol by box B. In one embodiment, the variable shared secret is 20 bits long, but this could be bootstrapped (if necessary, by iteration) to become a longer shared secret.

30 Either the fixed shared secret or the variable shared secret (or some combination of

the two) could be used as a one-time pad to encrypt the random plaintext along one-time-pad lines, in which both encryption and decryption are simple “exclusive or”.

In the remainder of this description, the 256-bit session key shall be used to
5 perform a Rijndael encryption of the random plaintext constituted by the 's' k_j .

3) ‘idB’ and ‘pubA’ (stored in permanent storage) lead to the construction of a session key ‘S’ for this one-time provision of the (self-destructive) computational ability of B to allow the player to display the film.
10

4) Session key IS’ allows the Is’ film-segment keys k_j $1 \leq j \leq s$, to be built up in temporary storage. They are encrypted and decrypted with session key ‘S’, using Rijndael. Since k_j at 256 bits is much smaller than a film segment, it may be possible to use a Rijndael key that is somewhat smaller than 256 bits. If Rijndael is used for both keys
15 and film, both the key-exchange module and the decryption module can call on the same Rijndael decryptor submodule.

5) “Tamper proof” means that both temporary and permanent storage will be wiped clean if anyone attempts to open the crypto module. “Super glue”, piezoelectric
20 techniques, and physical construction together provide layered strong box or “titanium-box” physical-security to the key-like material stored in box B.

Key-Exchange Protocol

25 A brief description of the key-exchange protocol, where A is the station and B is one of one million boxes registered with the station, is provided below. Standard notation is used. A and B are legitimate parties.

“A --> B: x” denotes the message x sent by A to B. Spoofing is possible so that B
30 does not normally know if the message was indeed from A.

“1. A --> B: x” denotes that which the protocol designer intended as the first message of the protocol. The trustworthiness of the external world cannot be assumed so this too must be independently verified.

5

“ $\{x\}_k$ ” means x encrypted under k.

“ $[x]_{k^{-1}}$ ” means x signed under k^{-1} the key that “inverts” k.

10 This notation recognises that the key pairs used in cryptosystems come in pairs, where one key allows encryption and the other key (the same key in symmetric-key systems) allows decryption. The private decryption key is used to generate digital signatures.

15 Implementation

Each key-exchange protocol step is followed by a description in simple English.

1. B --> A: {Step1 (B to A), movie, idB, numberB, MAC}pubA

20 Box B initiates one instance of the key-exchange protocol with Station A by sending him this message. Box B identifies the protocol step, the movie, and provides his genuinely-random 256-bit unique identification number ‘idB’.

‘NumberB’ is the number of times this box has initiated this key-exchange protocol.

25 ‘MAC’ is a message-authentication code implemented by a keyed hash function. The file is encrypted with station A’s quasi-public key ‘pubA’. ‘NumberB’ will be incremented by one before this protocol is invoked by box B again.

30 2. A --> B: <Step2 (A to B), elementA, numberB, MAC>

This message is sent in the clear with integrity and authentication checks. In particular, the message-authentication code (MAC) is $[h(m)]_{priA}$, that is the hash of the entire message preceding the MAC digitally signed by station A. 'NumberB' could be camouflaged if this is desired. 'ElementA' is randomly selected by station A as an element of the large cyclic group managed by A. When box B receives this message, it is either discarded or else allows box B to compute the session key $S = elementA^{bB}$. At this point, both station A and box B share the secret session key 'S', which is unavailable to anyone else even though 'elementA' was sent in the clear.

10 3. B --> A: {Step3 (B to A), ack}S

Box B acknowledges successful computation of session key 'S'.

4. A --> B: {Step4 (A to B), segment size, s}S

The station provides some information about the file.

15

5. A --> B: {Step5 (A to B), j, k_j }S, for $1 \leq j \leq s$.

The station transmits all 's' film-segment keys k_j to box B. Individual keys may be sent as separate messages or all keys may be sent as one long message. The conservative approach is to use a suitably-sized 'S' as a Rijndael key and encrypt each k_j , or the concatenation of all k_j , with the Rijndael algorithm.

20

6. B --> A: {Step6 (B to A), ack}S

Box B acknowledges successful termination of this instance of the key-exchange protocol. Upon recovery of all the fragment keys k_j , session key 'S' is destroyed.

25

Decryption of Digital Content

Box B has access to 's' encrypted film-segments c_j , $1 \leq j \leq s$. He also has access (possibly all at once, possibly just in time) to 's' Rijndael symmetric-key decryption keys k_j , $1 \leq j \leq s$. There is great flexibility at this point. Depending on the

30

ability to buffer within the decryption module, the segments may be decrypted in sequential order, in some other order, or even in parallel.

In the simplest case, the fragments will be decoded and sent in order to the player by secure cable. There is a clear division in time. When the box is free-standing from the player, the system guards the plaintext MPEG (in this example) signal until it enters the player through the digital input port. As soon as key k_j is used to decrypt segment c_j , k_j is destroyed.

10 Installation & Security of the Box

In one embodiment of the invention, the a customised cable is used to connect the crypto module to the subscriber's player. The box may be embedded inside the player. Any tampering with the cable or the connection to the digital input port causes a shutdown of the entire crypto module and the erasure of all permanent and temporary storage within the crypto module. A description of other features of the box follows.

1) In permanent box storage, 'idB' and 'bB' are protected with extreme care, that is the tamper-proof "titanium box" must guarantee that these two bit values cannot be captured even if the box is physically attacked.

2) The fragment keys k_j , $1 \leq k_j \leq s$ are protected. Their physical presence inside the crypto module is relatively brief. The session key 'S' is also quite sensitive. It can be used after the fact to recover the k_j .

3) It may be preferable to use distinct session keys to encrypt distinct segment keys. This could improve flexibility and efficiency, as well as increase security.

Although the present invention has been described in detail with reference to one or more preferred embodiments, persons possessing ordinary skill in the art to which this

invention pertains will appreciate that various modifications and enhancements may be made without departing from the scope of the claims that follow. The various alternatives for providing a highly secure data distribution system that have been disclosed above are intended to educate the reader about preferred embodiments of the invention and are not intended to constrain the limits of the invention or the scope of claims.

5

CLAIMS

1. A method of securing data transmitted to a user device from a content provider; including the steps of:
 - 5 providing for authentication of the user device;
 - encrypting a data file for transmission to the user device;
 - transmitting to the user device the data file and an encryption key specific to the transmission;
 - decrypting the data file; and
 - 10 destroying the encryption key.

2. A method according to claim 1, including the steps of:
 - dividing the data file into a plurality of segments;
 - assigning to each data segment a segment encryption key;
 - 15 transmitting to the user device the plurality of data segments and the plurality of segment encryption keys;

wherein the segment encryption keys are destroyed once each data segment has been decrypted.

- 20 3. A method according to claim 2, wherein the or each encryption key is destroyed immediately after decryption of the associated data segment.

4. A method according to claim 2 or 3, wherein each encryption key is destroyed prior to decryption of any other data segment.

- 25 5. A method according to any preceding claim, wherein the or each encryption key is useable within a predetermined time period.

6. A method according to any preceding claim, wherein the or each encryption
30 key is generated from an unpredictable and/or irreproducible number source.

7. A method according to claim 6, wherein the or each encryption key is produced from a random number source.

5 8. A method according to claim 7, wherein the random source is a white noise generator.

9. A method according to any preceding claim, wherein the or each encryption key is a 256-bit key.

10

10. A method according to any preceding claim, wherein the or each encryption key is a Rijndael key.

11. A method according to any preceding claim, wherein the user device is provided with a public encryption key for providing authentication of the user device.

15

12. A method according to any preceding claim, including the step of providing a session encryption key usable during a transmission session between the content provider and a user device.

20

13. A method according to any preceding claim, wherein authentication of a user device is carried out on the basis of short data signal.

14. A method according to claim 13, wherein the short data signal is a few bits in length.

25

15. A system for transmitting data securely to a user device from a content provider; including:

means operable to provide for authentication of the user device;

30

encryption means for encrypting a data file for transmission to the user device;

means for transmitting to the user device the data file and an encryption key specific to the transmission;

decryption means for decrypting the data file; and

means for destroying the encryption key.

5

16. A system according to claim 15, including:

means for dividing the data file into a plurality of segments;

means for assigning to each data segment a segment encryption key;

wherein the transmitting means is operable to transmit to the user device the

10 plurality of data segments and the plurality of segment encryption keys and the destroying means is operable to destroy the segment encryption keys once each data segment has been decrypted.

17. A system according to claim 16, wherein destroying means is operable to

15 destroy the or each encryption key immediately after decryption of the associated data segment.

18. A system according to claim 16 or 17, wherein the destroying means is operable to destroy each encryption key prior to decryption of any other data segment.

20

19. A system according to any one of claims 15 to 18, including an unpredictable and/or irreproducible number source generating the or each encryption key.

20. A system according to claim 19, wherein the unpredictable and/or

25 irreproducible number source is a random number source.

21. A system according to claim 20, wherein the random source is a white noise generator.

30 22. A system according to any one of claims 15 to 21, including means for

providing a session encryption key usable during a transmission session between the content provider and a user device.

23. A system according to any one of claims 15 to 22, wherein the user device is
5 provided with a memory for storage of authentication data which is destroyed upon physical opening or tampering of the device.

24. A system according to any one of claims 15 to 22, wherein the electronic
10 components of the user device are covered in a glue or potting compound.

25. A system according to any one of claims 15 to 24, including tamper
detection means for detecting tampering of the user device, the tamper detection means
being operable to erase all stored data in the user device upon the detection of tampering.

15 26. A system according to any one of claims 15 to 25, wherein the user device does not permanently store any of the encryption keys apart from a public encryption key.

20 27. A system according to any one of claims 15 to 26, wherein the user device and the content provider are operable to provide for the authentication of the user device on the basis of short data signal.

28. A system according to claim 27, wherein the short data signal is a few bits in length.

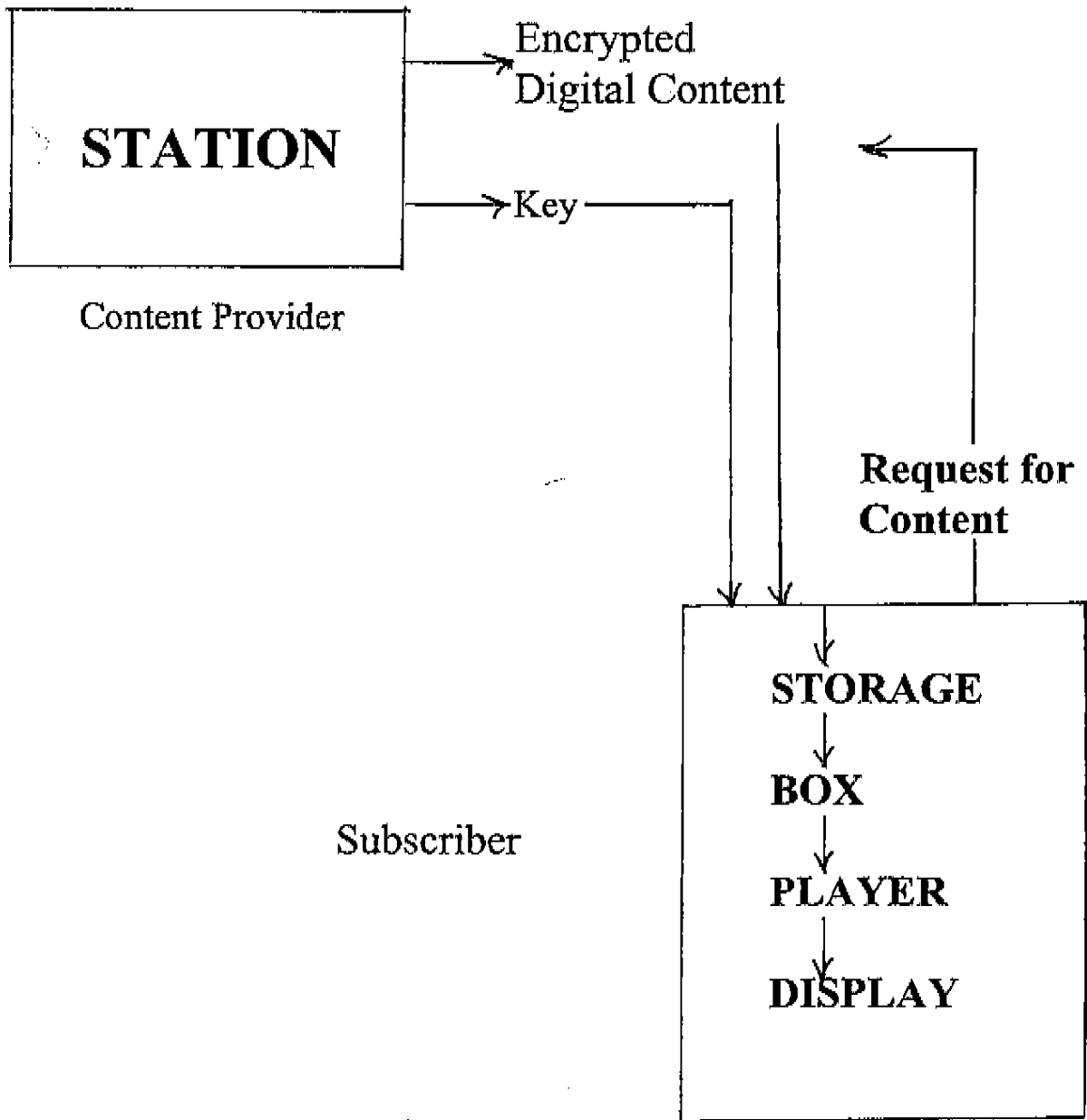
ABSTRACT5 METHOD AND APPARATUS FOR SECURE DELIVERY OF DATA

Methods and apparatus for the secure and copy-proof distribution of digital content are disclosed. In a preferred embodiment cryptographic primitives (encryption algorithms, message-authentication codes, hash functions, random-number generators, etc.) are used in a novel security protocol. The system may be utilised to protect a first-run movie that has been digitised in accordance with one of the current or forthcoming MPEG standards (e.g., MPEG-7). Content receivers or users first register their boxes. This registration information is stored in a secure database. When a subscriber registers, he/she then receives a box (interface to his player) that has been initialised to contain a number of tamper-proof secrets that are shared between the station and that particular box. The station stores an encrypted version of the digital content. This encrypted version ultimately arrives at some unprotected storage medium local to the player. Upon demand, the station delivers to the box the use-once computational ability to decrypt the content and display it on the player or terminal.

10
15
20

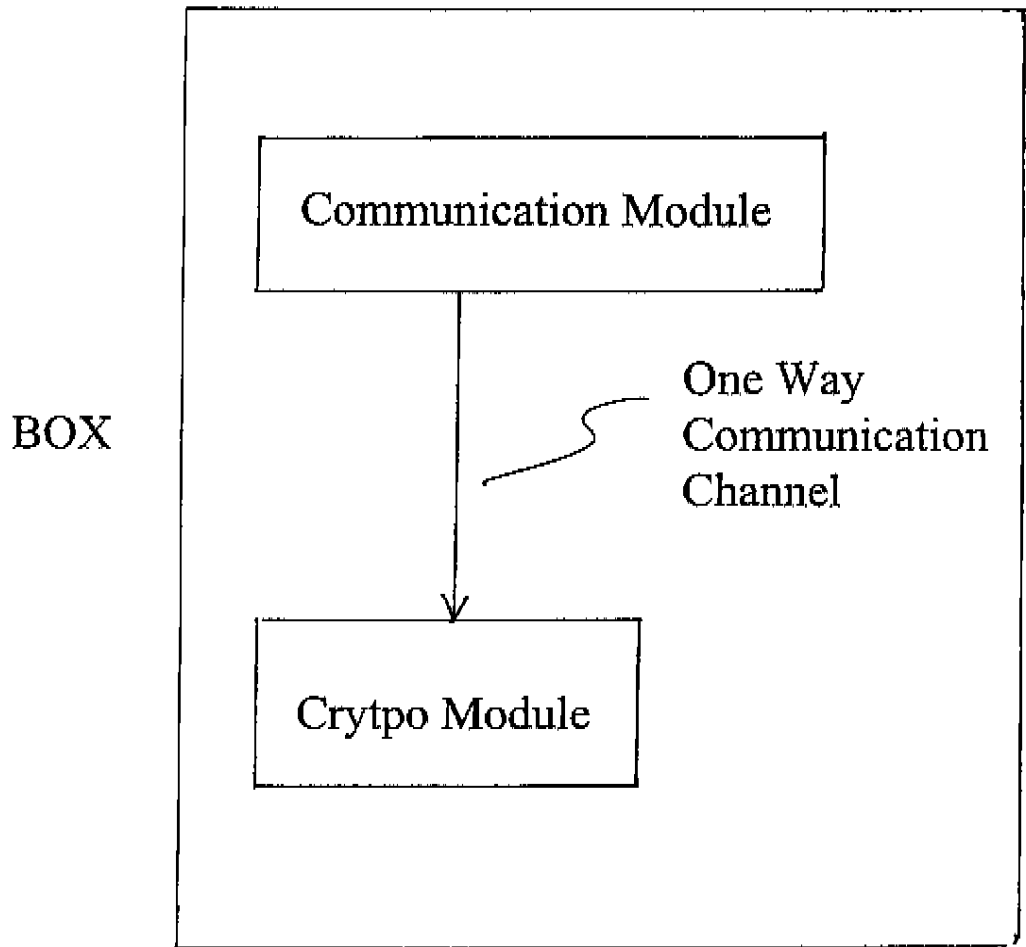
1/4

Figure 1



2/4

Figure 2



3/4

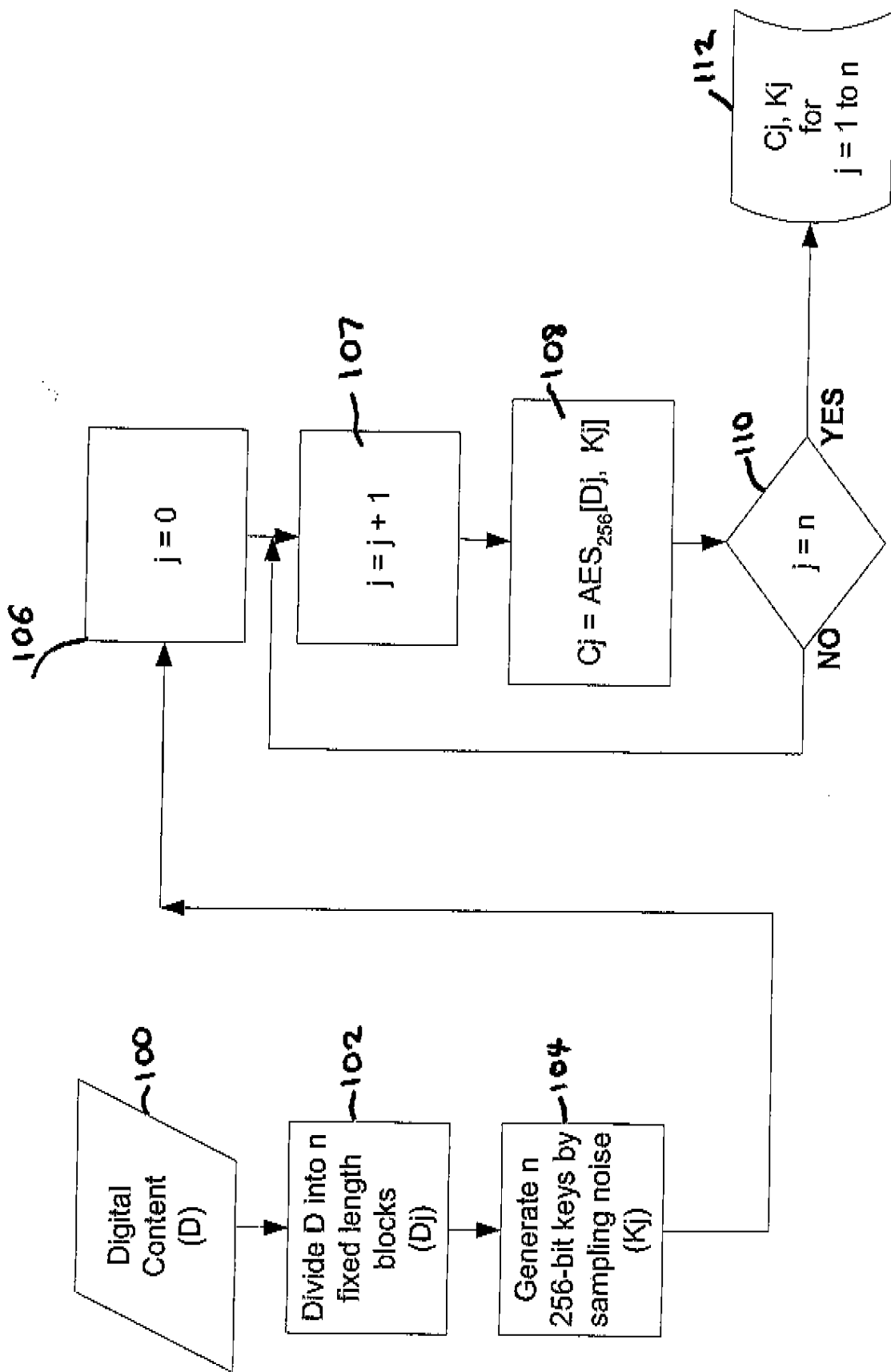


Fig. 3

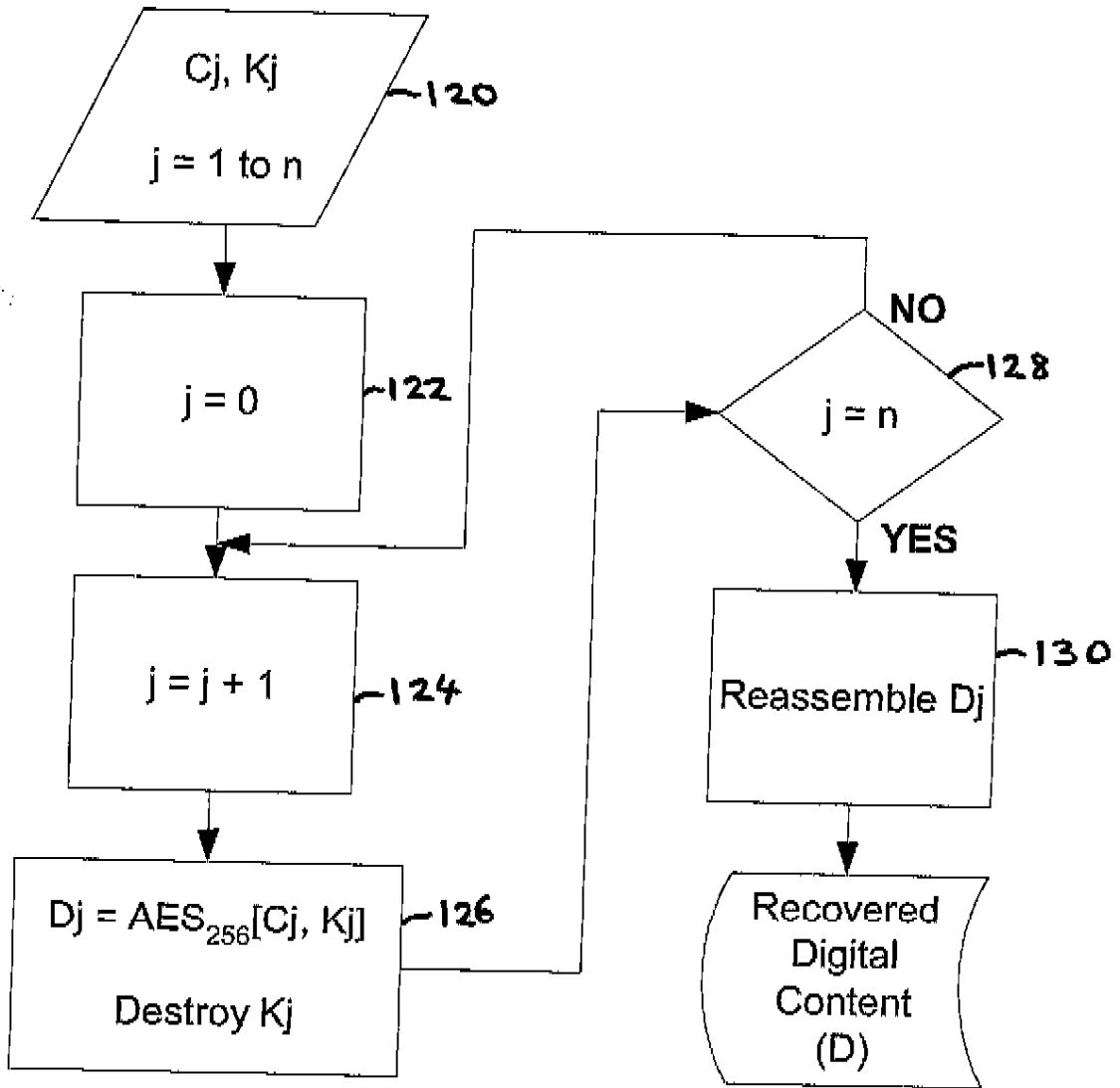


Fig. 4