

ITALIAN PATENT OFFICE

Document No.

102012902029839A1

Publication Date

20130908

Applicant

STMICROELECTRONICS S.R.L.

Title

MEZZO DI MEMORIZZAZIONE, LETTORE E METODO PER LEGGERE
CONTENUTI DEL MEZZO DI MEMORIZZAZIONE NEL LETTORE.

DESCRIZIONE

Campo di applicazione

La presente invenzione riguarda un mezzo di memorizzazione che memorizza almeno un contenuto, ad esempio un film, un contenuto
5 audio o dati, ed atto ad essere inserito in un lettore per leggere o riprodurre il contenuto. Più in particolare, l'invenzione riguarda un mezzo di memorizzazione del tipo descritto sopra, in cui i contenuti sono codificati per impedirne la copiatura o lettura. L'invenzione riguarda anche un lettore dei contenuti memorizzati nel mezzo di
10 memorizzazione ed un metodo per leggere tali contenuti nel lettore.

Tecnica nota

Com'è noto, un mezzo di memorizzazione quale ad esempio un CD, un DVD o un disco Blue-ray memorizza dati, ad esempio un film, una traccia audio, dati o altri dati in formato digitale, che possono
15 essere letti o riprodotti con un lettore come ad esempio un riproduttore CD, un riproduttore DVD o un riproduttore di dischi Blue-ray, atto a ricevere il mezzo di memorizzazione in una sede, che include ad esempio un motore elettrico per azionare il mezzo di memorizzazione per la lettura.

20 I dati in formato digitale hanno l'inconveniente di poter essere facilmente copiati da un mezzo di memorizzazione ad un altro, senza che i loro contenuti subiscano una degradazione, e ciò ai danni del diritto d'autore di un proprietario. La Figura 1 rappresenta schematicamente un mezzo di memorizzazione ed un lettore o
25 riproduttore. Il mezzo di memorizzazione 100 può essere caricato nel

riproduttore 110 e il riproduttore 110 riceve e decodifica i dati o il contenuto dal mezzo di memorizzazione 100.

Sono state implementate diverse tecniche per tentare di impedire una copia dei contenuti o la loro decodifica. Ad esempio, alcuni produttore di CD musicali hanno implementato un metodo per 5 disabilitare la copiatura dei dati contenuti nel mezzo di memorizzazione marcando le tracce audio con una chiave di cifratura memorizzata nel CD. I dati contenuti vengono marcati o cifrati dalla chiave nel CD. Tuttavia, un hacker può trovare dove viene memorizzata la chiave nei 10 mezzi di memorizzazione ed estrarre la chiave per decifrare facilmente i contenuti.

Il problema alla base della presente invenzione è quello di fornire un mezzo di memorizzazione che memorizzi un contenuto cifrato che non può essere usato per recuperare informazioni per decifrarlo, 15 anche se tale contenuto viene interamente copiato ed ispezionato in un altro dispositivo, superando in tal modo il problema che affligge attualmente i mezzi di memorizzazione della tecnica nota.

Sommario dell'invenzione

L'idea di soluzione alla base della presente invenzione è quella 20 di memorizzare le informazioni necessarie a decifrare i contenuti cifrati di un mezzo di memorizzazione in un dispositivo separato, in modo tale che queste informazioni non possano essere copiate insieme ai contenuti. Tale dispositivo separato è annesso al mezzo di memorizzazione e non può essere letto da una testina di lettura di un 25 lettore atto a riprodurre o leggere i contenuti del mezzo di

memorizzazione; le informazioni possono essere recuperate da un dispositivo specializzato del lettore.

Secondo l'idea di soluzione fornita sopra, il problema tecnico viene risolto da un mezzo di memorizzazione che memorizza almeno un
5 contenuto ed è atto ad essere inserito in un lettore per leggere il contenuto, caratterizzato dal fatto che il contenuto è cifrato ed il mezzo di memorizzazione comprende uno smart object attaccato fisicamente sul mezzo di memorizzazione e sistemato per essere letto da uno smart object reader del lettore, lo smart object comprendendo informazioni di
10 sicurezza per decifrare il contenuto nello smart object reader.

Vantaggiosamente, il contenuto non include le informazioni di sicurezza, queste ultime essendo memorizzate nello smart object e dunque una copiatura del contenuto dal mezzo di memorizzazione su un altro dispositivo non può includere tali informazioni di sicurezza.

15 In un aspetto dell'invenzione, lo smart object è incorporato in uno strato che ricopre una superficie del mezzo di memorizzazione ed è sostanzialmente complanare con lo strato per evitare interferenza meccanica nel lettore, lo strato essendo preferibilmente uno strato stampato. Vantaggiosamente, lo strato può essere fabbricato
20 separatamente dal mezzo di memorizzazione e successivamente attaccato ad una superficie del mezzo di memorizzazione; lo strato stampato può inglobare lo smart object. In un altro aspetto, lo smart object è attaccato con una colla sulla superficie del mezzo di memorizzazione.

25 Preferibilmente, la connessione evita un disaccoppiamento

dello smart object dal mezzo di memorizzazione; ad esempio, i componenti elettronici dello smart object si danneggiano se esso si stacca dal mezzo di memorizzazione, a causa del tipo di colla utilizzata oppure a causa del materiale dello strato stampato.

5 Il mezzo di memorizzazione è elettricamente scollegato dallo smart object. Sia il mezzo di memorizzazione che lo smart object sono elettricamente passivi. Vantaggiosamente, le informazioni di sicurezza nello smart object possono essere lette solo da un smart object reader ed usate per decifrare il contenuto se lo smart object reader comunica le
10 informazioni di sicurezza alla testina di lettura del riproduttore.

 In una forma di realizzazione dell'invenzione, il mezzo di memorizzazione comprende un CD, un DVD o un disco Blue-ray e lo smart object è attaccato su una superficie circolare del mezzo di memorizzazione. Vantaggiosamente, secondo questa forma di
15 realizzazione, una testina di lettura del lettore e intelligente dello smart object reader sono operative contemporaneamente su facce contrapposte del mezzo di memorizzazione. Inoltre, questa disposizione dello smart object reader consente di mantenere corrispondenza e retro-compatibilità con mezzi di memorizzazione e con lettori già
20 disponibili sul mercato.

 Lo smart object è preferibilmente attaccato vicino ad un centro della superficie avente una velocità lineare ridotta quando il mezzo di memorizzazione viene riprodotto. In un'altra forma di
realizzazione, lo smart object è attaccato in una porzione periferica del
25 mezzo di memorizzazione.

In un altro aspetto dell'invenzione, lo smart object comprende mezzi per comunicare senza contatto con lo smart object reader quando i mezzi di memorizzazione si muovono per la riproduzione, i mezzi essendo attivati elettricamente dallo smart object reader.

- 5 Vantaggiosamente, secondo questo aspetto, la comunicazione tra lo smart object reader e lo smart object è operativa anche quando il mezzo di memorizzazione viene attivato dal lettore per la lettura/riproduzione e dunque le informazioni di sicurezza necessarie per leggere e riprodurre possono essere recuperate dinamicamente, in fase di movimento. Tali
- 10 informazioni possono essere associate a porzioni differenti del mezzo di memorizzazione; dunque, un primo contenuto nel mezzo di memorizzazione da leggere può essere codificato con un primo algoritmo predeterminato ed una prima chiave di cifratura, i quali sono memorizzati nello smart object e trasmessi allo smart object reader
- 15 quando il lettore riceve una richiesta di lettura o riproduzione del primo contenuto; un altro contenuto nel mezzo di memorizzazione può essere cifrato con un altro algoritmo ed un'altra chiave di cifratura, diversi dal primo algoritmo e dalla prima chiave di cifratura, che sono memorizzati nello smart object e trasmessi allo smart object reader quando il
- 20 riproduttore riceve una richiesta di lettura o riproduzione di detto altro contenuto.

Le informazioni di sicurezza sono trasmesse dallo smart object reader al lettore senza interruzione del movimento del mezzo di memorizzazione nel lettore.

- 25 In un aspetto dell'invenzione, nel mezzo di memorizzazione

risulta definita una pluralità di sezioni, in cui una o più sezioni protette di dette sezioni sono associate ad una o più corrispondenti informazioni di sicurezza. In una forma di realizzazione, un gruppo di sezioni protette può anche essere associato a singole informazioni di sicurezza. Lo smart
5 object reader può recuperare informazioni di sicurezza su tali diverse sezioni protette mentre il lettore sta muovendo il mezzo di memorizzazione.

Le informazioni di sicurezza comprendono mezzi per decifrare i contenuti cifrati, ad esempio una chiave di cifratura e/o un algoritmo
10 di cifratura e/o parametri di chiave per l'algoritmo di cifratura. Lo smart object comprende una scheda per circuito integrato o una smart card che soddisfano la specifica ISO 7816.

In un aspetto dell'invenzione, il mezzo di memorizzazione comprende una pluralità di sezioni associate alle informazioni di
15 sicurezza. Lo smart object è programmato per ricevere dallo smart object reader una richiesta delle informazioni di sicurezza su una sezione protetta da leggere o riprodurre e per restituire le informazioni di sicurezza allo smart object reader, per decifrare il contenuto della sezione protetta.

20 In un altro aspetto dell'invenzione, un produttore di contenuti da memorizzare nel mezzo di memorizzazione ed un produttore del lettore si accordano sulle chiavi di cifratura e decifratura e sugli algoritmi di cifratura. Successivamente, il produttore di contenuti cifra i suoi contenuti usando l'algoritmo e le chiavi di cifratura e memorizza i
25 contenuti cifrati nel mezzo di memorizzazione; tali chiavi ed algoritmi

non vengono memorizzati nel mezzo di memorizzazione bensì nello smart object, sotto forma di informazioni di sicurezza; ad esempio, dette informazioni vengono memorizzate in una posizione di memoria dello smart object che viene comunicata al lettore. Il produttore di lettore
5 programma lo smart object reader per l'accesso alle informazioni di sicurezza precedentemente concordate con il produttore di contenuti, ad esempio accedendo alla posizione di memoria e leggendo le informazioni di sicurezza, per decifrare i contenuti.

Il problema tecnico sopra descritto viene anche risolto da un
10 lettore per leggere almeno un contenuto memorizzato in un mezzo di memorizzazione atto ad essere inserito nel lettore. Uno smart object reader è integrato nel lettore ed è atto a leggere informazioni di sicurezza da uno smart object che è fisicamente attaccato al mezzo di memorizzazione, le informazioni di sicurezza essendo utilizzate dallo
15 smart object reader per decifrare il contenuto.

In un aspetto dell'invenzione, lo smart object reader è programmato per richiedere le informazioni di sicurezza allo smart object reader su almeno una sezione protetta del mezzo di memorizzazione e per ricevere dallo smart object le informazioni di
20 sicurezza per decifrare il contenuto della sezione protetta.

Il problema alla base dell'invenzione viene anche risolto da un metodo per proteggere un contenuto memorizzato in un mezzo di memorizzazione che è atto ad essere inserito in un lettore per la lettura; il metodo comprende le fasi di trasmettere una interrogazione da uno
25 smart object reader integrato nel lettore ad uno smart object attaccato

al mezzo di memorizzazione e sistemato per essere letto dal lettore, per recuperare un'informazione di sicurezza per decifrare il contenuto nello smart object reader.

Si prevede un'ulteriore fase di identificare una sezione protetta
5 del mezzo di memorizzazione che memorizza il contenuto ed una fase di richiedere le informazioni di sicurezza per decifrare il contenuto della sezione protetta.

Ulteriori vantaggi e caratteristiche del metodo, del lettore e del mezzo di memorizzazione secondo la presente invenzione risulteranno
10 evidenti dalla descrizione fornita qui di seguito solo a scopo esemplificativo e senza limitare l'ambito di protezione della presente invenzione.

Breve descrizione dei disegni

La Figura 1 rappresenta schematicamente un mezzo di
15 memorizzazione ed un lettore secondo la tecnica nota.

La Figura 2A rappresenta schematicamente un mezzo di memorizzazione ed un lettore secondo l'invenzione.

La Figura 2B rappresenta schematicamente in una vista ingrandita il mezzo di memorizzazione di Figura 2A.

20 La Figura 3 rappresenta schematicamente uno scambio di dati tra il mezzo di memorizzazione che include uno smart object ed il riproduttore che include uno smart object reader secondo l'invenzione.

La Figura 4 rappresenta schematicamente sezioni di un mezzo di memorizzazione secondo l'invenzione.

25 Descrizione dettagliata

Con riferimento alla figura 2A, un mezzo di memorizzazione che memorizza uno o più contenuti, ad esempio film, tracce audio o altri dati in formati predeterminati, ad esempio un CD, un DVD oppure un Blue-ray, viene rappresentato schematicamente ed indicato con 100. I
5 dati vengono cifrati per proteggerli da una copiatura o una lettura non autorizzata in un lettore o riproduttore atto a ricevere il CD, DVD o Blue-ray in una rispettiva sede e ad azionarlo per la riproduzione.

Secondo la presente invenzione, il mezzo di memorizzazione comprende uno smart object che include informazioni per decifrare il
10 contenuto ed il lettore comprende uno smart object reader per leggere le informazioni nello smart object . Con riferimento alla figura 2B, il mezzo di memorizzazione 100 comprende uno smart object 200 fisicamente attaccato al mezzo di memorizzazione 100, ad esempio su un lato contrapposto rispetto ad un lato inciso o di memorizzazione del mezzo
15 di memorizzazione, quest'ultimo lato essendo accoppiato ad una testina di lettura del lettore che legge il contenuto.

Lo smart object è un hardware separato rispetto al mezzo di memorizzazione, ossia un dispositivo avente una propria memoria ed un proprio microprocessore ed è fisicamente attaccato con una colla
20 oppure incorporato in o coperto da uno strato del lato del mezzo di memorizzazione, ad esempio uno strato stampato. Più in particolare, una superficie dello smart object è sostanzialmente complanare con una superficie dello strato che ricopre il mezzo di memorizzazione e non interferisce meccanicamente con la sede del lettore quando il mezzo di
25 memorizzazione è inserito nella sede e riprodotto.

In un aspetto dell'invenzione, lo smart object è attaccato in prossimità di un centro del dispositivo, quest'ultimo essendo ad esempio un supporto circolare con un foro centrale destinato ad essere inserito su una cerniera del lettore.

5 Più in particolare, lo smart object 200 è posizionato per essere letto dallo smart object 220 quando il mezzo di memorizzazione viene inserito nel lettore, ad esempio contrapposto alla testina di lettura del lettore, rispetto al mezzo di memorizzazione. In altre parole, una prima faccia del mezzo di memorizzazione comprende tracce e settori in cui i
10 contenuti vengono memorizzati in un formato codificato in digitale e lo smart object è attaccato sulla seconda faccia del mezzo di memorizzazione. La testina di lettura del lettore è rivolta verso la prima faccia e lo smart object reader è rivolto verso la seconda faccia del mezzo di memorizzazione.

15 In un aspetto dell'invenzione, lo smart object è una scheda per circuito integrato oppure una smart card che soddisfano la specifica ISO 7816 e lo smart object reader è un lettore di scheda per circuito integrato per la lettura della scheda per circuito integrato. Lo smart object 200 fornisce informazioni di sicurezza allo smart object reader
20 220 per decifrare il contenuto che, come menzionato sopra, è memorizzato in un formato cifrato nel mezzo di memorizzazione.

In un aspetto dell'invenzione, una comunicazione tra lo smart object ed il corrispondente smart object reader è senza contatto. Secondo questo aspetto, lo smart object reader legge lo smart object
25 anche quando il mezzo di memorizzazione si muove per una

riproduzione da parte del lettore. Più in particolare, lo smart object reader 220 ed il lettore possono essere prodotti in due hardware separati, collegati assieme, oppure come un singolo hardware che integra sia la funzione di comunicazione con lo smart object sia quella
5 di lettura del contenuto del mezzo di memorizzazione.

In un altro aspetto dell'invenzione, lo smart object reader entra in contatto con lo smart object per leggere le informazioni di sicurezza e dunque il mezzo di memorizzazione viene arrestato dal lettore per leggere le informazioni di sicurezza. Secondo questo aspetto
10 dell'invenzione, il lettore rileva una richiesta di lettura di una porzione o settore cifrato del mezzo di memorizzazione e lo arresta per leggere le informazioni di sicurezza, se viene rilevata una siffatta richiesta. In tale forma di realizzazione, lo smart object è preferibilmente attaccato ad una porzione periferica del mezzo di memorizzazione.

15 Le informazioni di sicurezza comprendono mezzi per decifrare il contenuto cifrato, ad esempio una chiave di cifratura, un algoritmo di cifratura o parametri di chiave per l'algoritmo.

La Figura 3 rappresenta schematicamente in un diagramma di flusso uno scambio di dati tra il mezzo di memorizzazione, lo smart
20 object, e lo smart object reader secondo l'invenzione.

Il mezzo di memorizzazione 100 viene inserito e caricato nel lettore 210 e comprende lo smart object 200 attaccato fisicamente. Lo smart object 200 scambia dati 300, 310 con lo smart object reader 220 ed il contenuto cifrato 320 del mezzo di memorizzazione viene fornito in
25 uscita al lettore 210. Più in particolare, lo smart object 200 trasmette

allo smart object reader 220 le informazioni di sicurezza 310 usate per decifrare il contenuto nel lettore, ossia i dati cifrati 320.

Le informazioni di sicurezza sono richieste dallo smart object reader 220 per una sezione protetta su cui legge un lettore 210. Tale
5 richiesta è sotto forma di una interrogazione 300 che include un'identificazione di settore.

Con riferimento alla figura 4, il mezzo di memorizzazione, ad esempio un mezzo di memorizzazione ottico, include sezioni che sono definite da un numero di cerchi, ciascun cerchio essendo
10 contraddistinto da un diametro diverso, ed una linea di divisione da un centro verso una circonferenza del cerchio. Ad esempio, un primo settore 400 è circondato da due linee di divisione 450, 451 e da due cerchi 452, 453. Un secondo settore 410 può essere definito in un metodo simile.

15 In altre parole, secondo l'invenzione, il mezzo di memorizzazione 100 comprende una pluralità di sezioni 400, 410 associate a corrispondenti informazioni di sicurezza. Lo smart object reader trasmette allo smart object 200 una interrogazione 300 per le informazioni di sicurezza, che include un'identificazione di sezione, e lo
20 smart object 200 restituisce le informazioni di sicurezza 310 della sezione. Le informazioni di sicurezza 310 possono includere la chiave di cifratura/decifratura per la corrispondente sezione. In una forma di realizzazione dell'invenzione, si utilizzano informazioni di sicurezza predeterminate per specificare che una corrispondente sezione del
25 riproduttore non è protetta. In altre parole, per leggere il contenuto è

sempre necessaria una comunicazione tra lo smart object ed lo smart object reader, anche se la corrispondente sezione non è protetta, ma le informazioni di sicurezza trasmesse per tale sezione, dallo smart object allo smart object reader, non comprendono effettivamente alcun
5 algoritmo o chiavi di decifratura. Qualora inclusa nelle informazioni di sicurezza, lo smart object reader 220 estrae la chiave di cifratura/decifratura 310 e trasmette la chiave 330 al riproduttore 210. Il riproduttore 210 usa la chiave per decifrare e cifrare i dati 320. Vantaggiosamente, la chiave può essere diversa per ciascun diverso
10 formato dati, per ciascuna specifica traccia audio, video o altro formato dati. Il riproduttore 210 richiede la chiave di cifratura allo smart object reader, inviando il segnale 320 che include l'identificazione di sezione.

In una forma di realizzazione, le informazioni di sicurezza 310 comprendono l'algoritmo per cifrare/decifrare il contenuto in una
15 sezione protetta. Lo smart object reader 220 estrae la chiave e l'algoritmo di cifratura/decifratura 310 e trasmette la chiave e l'algoritmo di cifratura 330 al riproduttore 210, quest'ultimo utilizzando l'algoritmo e la chiave per decifrare i dati cifrati 320, ossia il contenuto protetto. In questo caso, sia la chiave che l'algoritmo possono essere
20 diversi per ciascun diverso formato dati, ossia per dati audio, video o ausiliari.

Secondo una forma di realizzazione dell'invenzione, una pluralità di sezioni vengono raggruppate insieme ed associate ad una medesima chiave e/o algoritmo. Ad esempio, vengono raggruppate tutte
25 le sezioni in un perimetro con una stessa distanza da un centro.

Vantaggiosamente, secondo questa forma di realizzazione, l'interrogazione per le informazioni di sicurezza può essere eseguita meno frequentemente poiché è possibile usare le stesse informazioni di sicurezza per decifrare più sezioni.

- 5 Vantaggiosamente, le informazioni di sicurezza sono memorizzate nello smart object 200 che è un dispositivo fisicamente separato dal mezzo di memorizzazione e dunque le informazioni di sicurezza non possono essere copiate con il contenuto memorizzato nel mezzo di memorizzazione. Ad uno smart object reader 220 con diritto di
- 10 accesso allo smart object viene richiesto di leggere le informazioni di sicurezza e di riprodurre il contenuto. Inoltre, memorizzando algoritmi e chiavi di cifratura/decifratura diversi per diverse sezioni del mezzo di memorizzazione, è possibile migliorare ulteriormente la protezione.



Ing. Mario BOTTI
N. Iscr. ALBO 493 BM

RIVENDICAZIONI

1. Mezzo di memorizzazione (100) per memorizzare almeno un contenuto ed atto ad essere inserito in un lettore per leggere il contenuto, caratterizzato dal fatto che detto contenuto è cifrato ed il
5 mezzo di memorizzazione comprende uno smart object (200) attaccato fisicamente sul mezzo di memorizzazione e sistemato per essere letto da uno smart object reader (220) di detto lettore, lo smart object (200) comprendendo informazioni di sicurezza (310) per decifrare detto contenuto nello smart object reader (220).

10 2. Mezzo di memorizzazione secondo la rivendicazione 1, in cui lo smart object è incorporato in uno strato che ricopre una superficie di detto mezzo di memorizzazione ed è sostanzialmente complanare con detto strato per evitare un'interferenza meccanica nel lettore, detto strato essendo preferibilmente uno strato stampato.

15 3. Mezzo di memorizzazione secondo la rivendicazione 1, in cui detto smart object è elettricamente scollegato dal mezzo di memorizzazione.

4. Mezzo di memorizzazione secondo le rivendicazioni 1-3, in cui il mezzo di memorizzazione comprende CD, DVD o un disco Blue-
20 ray e lo smart object è attaccato su una superficie circolare del mezzo di memorizzazione, detta superficie essendo opposta ad una superficie di incisione o di memorizzazione e lo smart object essendo preferibilmente attaccato in prossimità di un centro di detta superficie avente una velocità lineare minore quando il mezzo di memorizzazione viene
25 riprodotto.

5. Mezzo di memorizzazione secondo la rivendicazione 1, in cui lo smart object comprende mezzi di comunicazione senza contatto con lo smart object reader, quando il mezzo di memorizzazione si muove per essere riprodotto, detti mezzi essendo attivati elettricamente da
5 detto smart object reader.

6. Mezzo di memorizzazione secondo la rivendicazione 1, in cui le informazioni di sicurezza comprendono mezzi per decifrare i contenuti cifrati, detti mezzi comprendendo una chiave di cifratura e/o un algoritmo di cifratura e/o parametri chiave per l'algoritmo di
10 cifratura.

7. Mezzo di memorizzazione secondo la rivendicazione 1, in cui lo smart object comprende una scheda per circuito integrato o una smart card che soddisfano la specifica ISO 7816.

8. Mezzo di memorizzazione (100) secondo la rivendicazione
15 1, comprendente una pluralità di sezioni associate a corrispondenti informazioni di sicurezza (310).

9. Mezzo di memorizzazione (100) secondo la rivendicazione 8, in cui una o più sezioni protette sono raggruppate per essere associate a medesime informazioni di sicurezza.

20 10. Lettore per leggere almeno un contenuto memorizzato in un mezzo di memorizzazione (100) atto ad essere inserito nel lettore, caratterizzato dal comprendere uno smart object reader (220) integrato nel lettore ed atto a leggere informazioni di sicurezza (310) da uno smart object (200) che è fisicamente attaccato al mezzo di memorizzazione
25 (100), dette informazioni di sicurezza (310) essendo usate dallo smart

object reader (220) per decifrare il contenuto.

11. Lettore secondo la rivendicazione 10, in cui lo smart object reader (220) è programmato per richiedere dette informazioni di sicurezza (310) allo smart object (200) su almeno una sezione protetta
5 del mezzo di memorizzazione e per ricevere dallo smart object (200) le informazioni di sicurezza (310) per decifrare il contenuto di detta sezione protetta.

12. Lettore secondo la rivendicazione 11, caratterizzato dal comprendere una testina di lettura atta ad essere operativa
10 contemporaneamente allo smart object reader su facce contrapposte del mezzo di memorizzazione.

13. Metodo per proteggere un contenuto memorizzato in un mezzo di memorizzazione (100) che è atto ad essere inserito in un lettore per la lettura, caratterizzato dal comprendere le fasi di trasmettere una
15 interrogazione da uno smart object reader (220) integrato in detto lettore ad uno smart object (200) attaccato a detto mezzo di memorizzazione e sistemato per essere letto dal lettore, per recuperare informazioni di sicurezza (310) per decifrare detto contenuto nello smart object reader (220).

20 14. Metodo secondo la rivendicazione 13, comprendente le fasi di identificare una sezione protetta di detto mezzo di memorizzazione che memorizza il contenuto e richiedere le informazioni di sicurezza per decifrare il contenuto di detta sezione protetta.

15. Metodo secondo la rivendicazione 14, caratterizzato dal
25 comprendere la fase di memorizzare detto contenuto in un CD, un DVD

INC072BIT
STMicroelectronics S.r.l.

Ing. Mario Botti
(Iscr. Albo n. 493 BM)

o un disco Blue-ray come mezzo di memorizzazione.



Ing. Mario BOTTI
N. Iscr. ALBO 493 BM

RIVENDICAZIONI

1. A media storage (100) storing at least one content and adapted to be inserted in a media reader for reading the content, characterized by the fact that said content is encrypted and the media
5 storage comprises a smart object (200) physically attached on the media storage and arranged to be read by a smart object reader (220) of said media reader, the smart object (200) comprising a security information (310) for decrypting said content in the smart object reader (220).

2. Media storage according to claim 1, wherein the smart
10 object is embedded in a layer covering a surface of said media storage and is substantially coplanar with said layer to avoid mechanical interference in the media reader, said layer being preferably a printed payer.

3. Media storage according to claim 1, wherein said smart
15 object is electrically disconnected from the media storage.

4. Media storage according to claims 1-3, wherein the media storage comprises a CD, DVD or Blue-ray disc and the smart object is attached on a rounded surface of the media storage, said surface being opposite to a burning or storage surface, and the smart object being
20 preferably attached near to a center of said surface having a lower linear speed when the media storage is played.

5. Media storage according to claim 1, wherein the smart object comprises means for contactless communicating with the smart object reader, when the media storage is moved for playing, said means
25 being electrically activated by said smart card reader.

6. Media storage according to claim 1, wherein the security information comprises means for decrypting the encrypted content, said means comprising an encryption key and/or an encryption algorithm and/or key parameters for the encryption algorithm.

5 7. Media storage according to claim 1, wherein the smart object comprises an IC Card or a smart card complying with the ISO 7816 specification.

8. The media storage (100) according to claim 1 comprising a plurality of sections associated to corresponding security information
10 (310).

9. The media storage (100) according to claim 8, wherein one or more protected sections are grouped to be associated to a same security information.

10. A media reader for reading at least one content stored in
15 a media storage (100) adapted to be inserted in the media reader, characterized by comprising a smart object reader (220) integrated in the media reader and adapted to read a security information (310) from a smart object (200) which is physically attached to the media storage (100), said security information (310) being used from the smart object
20 reader (220) for decrypting the content.

11. The media reader according to claim 10, wherein the smart object reader (220) is programmed to requests said security information (310) to the smart object (200) on at least one protected section of the media storage and to receive from the smart object (200)
25 the security information (310) for decrypting the content of said

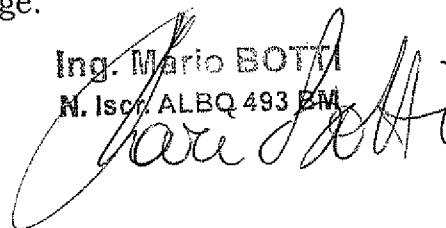
protected section.

12. Media reader according to claim 11, characterized by comprising a reading head which adapted to be contemporarily operative with the smart object reader on counter posed sides of the
5 media storage.

13. Method for protecting a content stored in a media storage (100) which is adapted to be inserted in a media reader for reading, characterized by comprising the steps of sending a query from a smart object reader (220) integrated in said media reader to a smart object
10 (200) attached to said media storage and arranged to be read from the media reader, for retrieving a security information (310) for decrypting said content in the smart object reader (220).

14. The method according to the claim 8 comprising the steps of identifying a protected section of said media storage which
15 stores the content and requesting the security information for decrypting the content of said protected section.

15. The method according to the claim 9, characterized by comprising the step of storing said content in a CD or DVD or and Blue-ray disc as a media storage.

Ing. Mario BOTTI
N. Iscr. ALBQ 493 BM


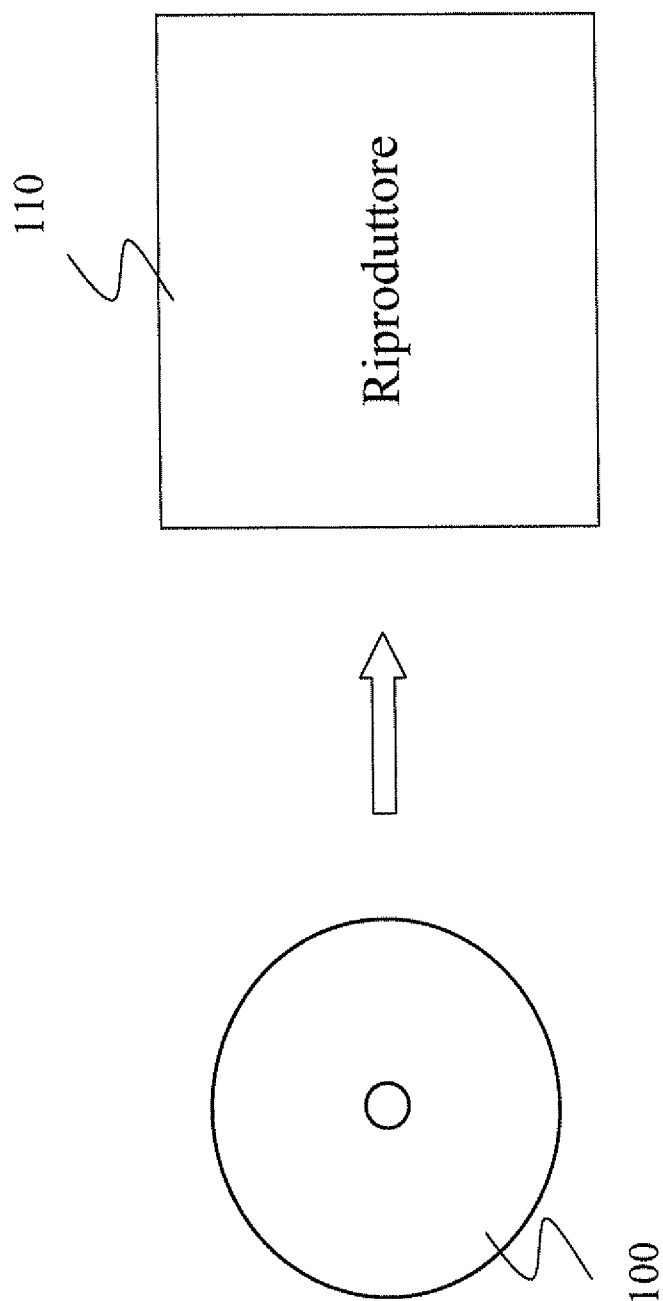


FIG. 1

Mario Botti
Ing. Mario BOTTI
N. Iscr. ALBO 493 BM

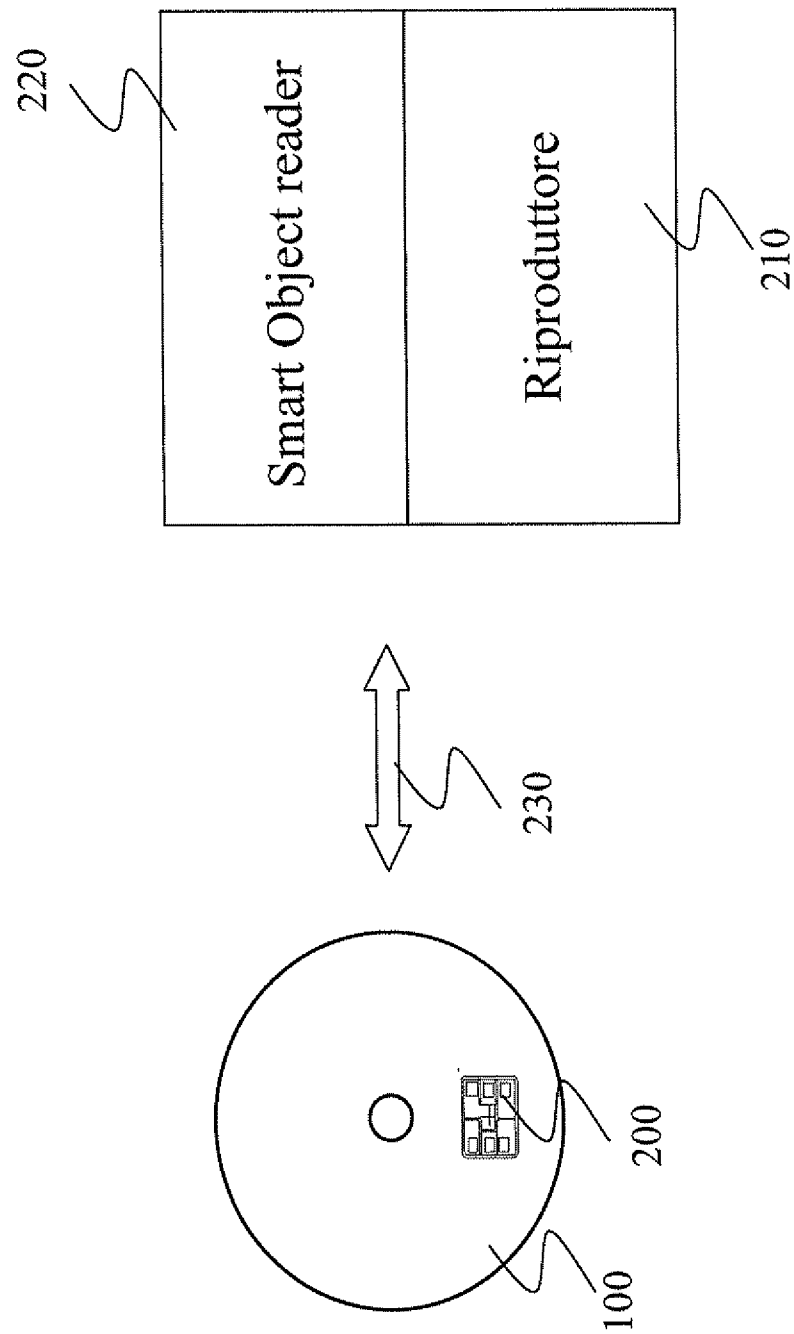


FIG. 2A

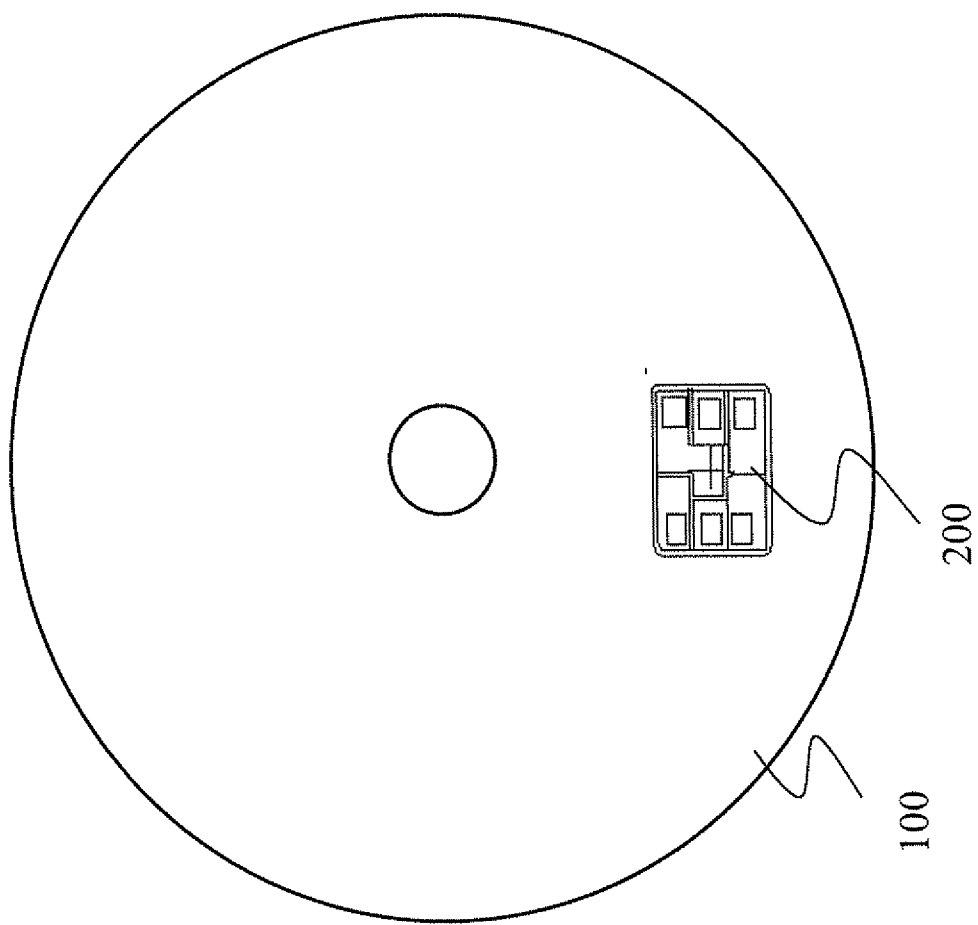


FIG. 2B

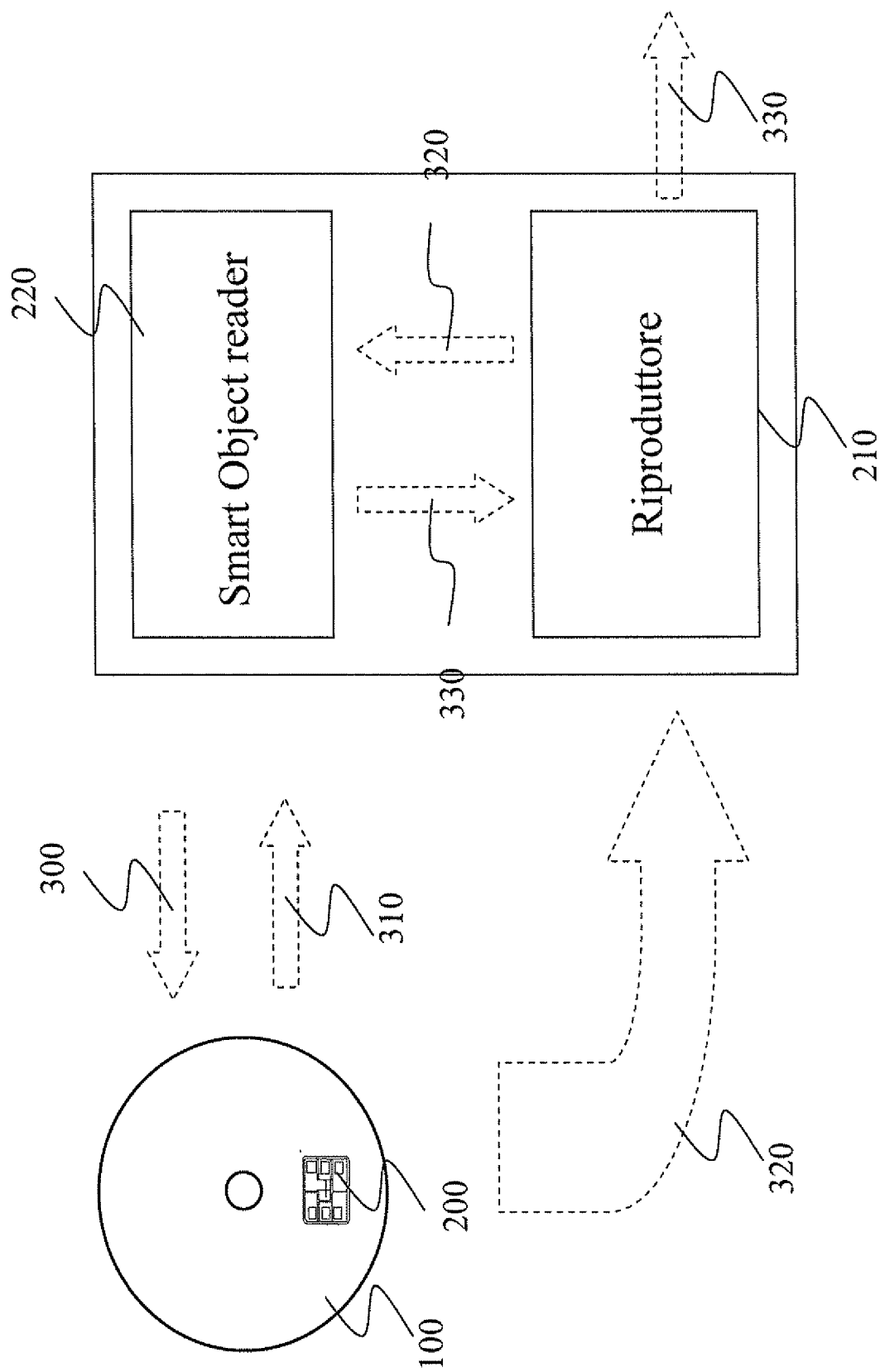


FIG. 3

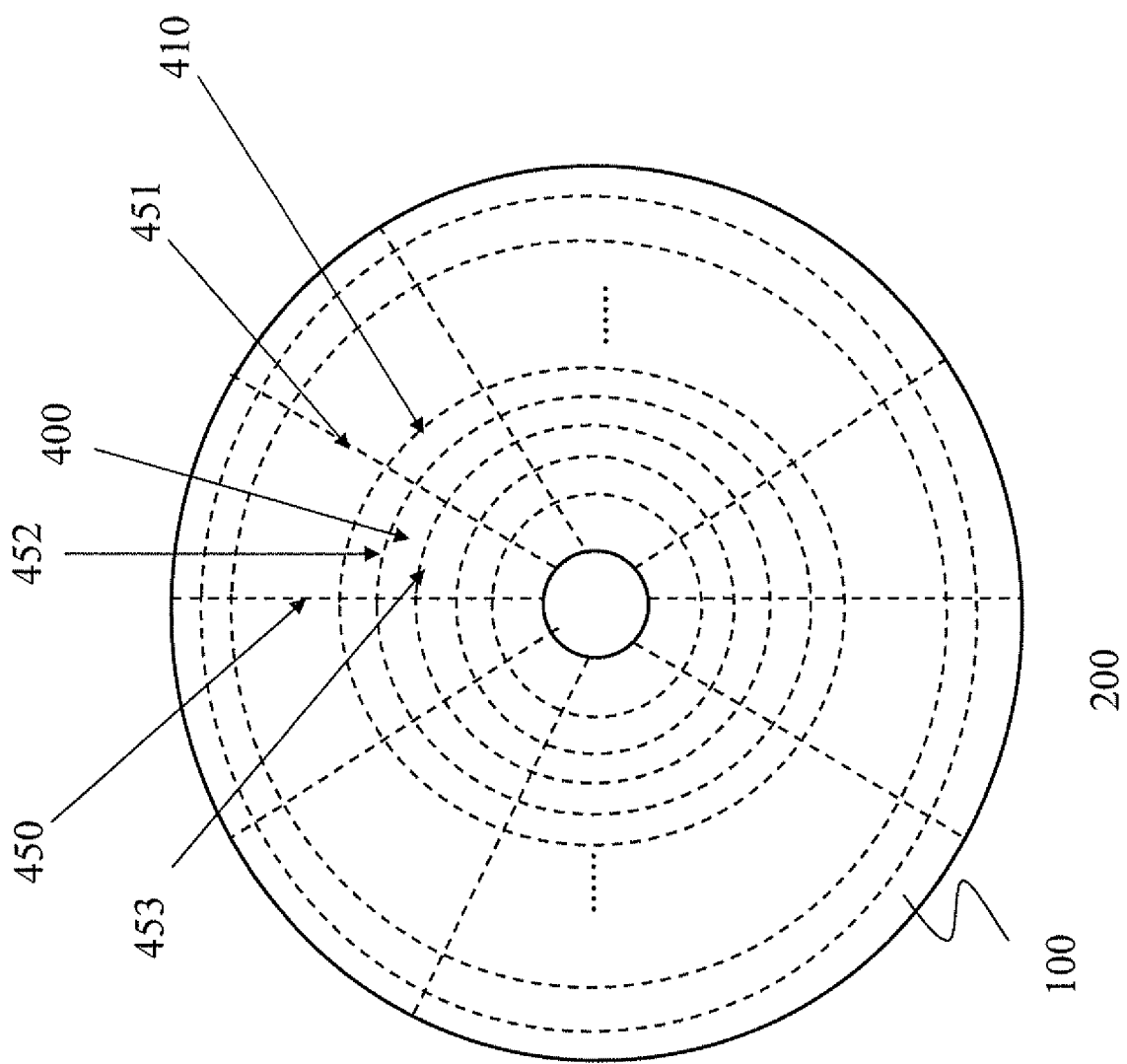


FIG. 4