(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7515751号
(P7515751)

(45)発行日　令和6年7月12日(2024.7.12)

(24)登録日　令和6年7月4日(2024.7.4)

(51)国際特許分類		FI		
H04L 9/08 (2006.01)		H04L	9/08	C
G06F 21/60 (2013.01)		G06F	21/60	320
H04L 9/32 (2006.01)		H04L	9/08	F
		H04L	9/32	200B

請求項の数　6　（全22頁）

(21)出願番号　特願2023-571699(P2023-571699)
(86)(22)出願日　令和4年5月16日(2022.5.16)
(65)公表番号　特表2024-518798(P2024-518798A)
(43)公表日　令和6年5月2日(2024.5.2)
(86)国際出願番号　PCT/CN2022/093116
(87)国際公開番号　WO2022/242607
(87)国際公開日　令和4年11月24日(2022.11.24)
審査請求日　令和5年11月17日(2023.11.17)
(31)優先権主張番号　202110546576.8
(32)優先日　令和3年5月19日(2021.5.19)
(33)優先権主張国・地域又は機関
中国(CN)
早期審査対象出願

(73)特許権者　508219313
杭州海康威視数字技術股▲フン▼有限公司
中華人民共和国浙江省杭州市濱江区阡陌路５５５号
(74)代理人　100110364
弁理士　実広 信哉
(74)代理人　100133400
弁理士　阿部 達彦
(72)発明者　王 ▲濱▼
中華人民共和国３１００５１浙江省杭州市▲濱▼江区阡陌路５５５号
(72)発明者　▲陳▼ 思
中華人民共和国３１００５１浙江省杭州市▲濱▼江区阡陌路５５５号

最終頁に続く

(54)【発明の名称】　ビデオデータスライスの暗号化方法、装置、システム及び電子デバイス

(57)【特許請求の範囲】

【請求項１】

鍵管理システムと複数の暗号化ノードとを含むビデオデータスライスの暗号化システムにおけるターゲット暗号化ノードに適用されるビデオデータスライスの暗号化方法であって、前記ターゲット暗号化ノードは前記複数の暗号化ノードのいずれかであり、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスは、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、

前記ターゲット暗号化ノードが第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するステップと、

前記ターゲット暗号化ノードが第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るステップと、

前記ターゲット暗号化ノードが前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るステップと、

前記ターゲット暗号化ノードが前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するステップと、を含み、

ここで、ビデオ鍵はビデオデータスライスを暗号化するために用いられ、保護鍵はビデオ鍵を暗号化するために用いられ、前記第１の保護鍵は、前記ターゲット暗号化ノードの検証に合格した場合に、前記鍵管理システムによって前記ターゲット暗号化ノードに送信され、同じ鍵ＩＤに対応する保護鍵は同じであり、

前記ターゲット暗号化ノードが前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するステップは、
前記ターゲット暗号化ノードが第２の乱数を生成し、前記第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成するステップと、
前記ターゲット暗号化ノードが前記ターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズムを用いて、前記ターゲット暗号化ノードのデバイスＩＤ、前記第１の鍵ＩＤ、及び前記鍵パラメータに署名し、第１の署名データを得るステップと、
前記ターゲット暗号化ノードが前記デバイスＩＤ、前記第１の鍵ＩＤ、前記鍵パラメータ、及び前記第１の署名データを前記鍵管理システムに送信することにより、前記鍵管理システムに、前記デバイスＩＤに基づいて前記ターゲット暗号化ノードの公開鍵を取得させ、前記ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて前記第１の署名データを検証させ、検証に合格した場合、第３の鍵に基づいて、前記第１の鍵ＩＤに対応する前記第１の保護鍵を暗号化させ、保護鍵暗号文を得させるステップであって、前記第３の鍵は、前記鍵管理システムによって、前記鍵パラメータと前記鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて生成される、ステップと、
前記ターゲット暗号化ノードが前記鍵管理システムから送信された前記保護鍵暗号文を受信するステップと、
前記ターゲット暗号化ノードが前記鍵管理システムの公開鍵と前記第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成するステップと、
前記ターゲット暗号化ノードが前記第４の鍵に基づいて前記保護鍵暗号文を復号化し、前記第１の保護鍵を得るステップと、を含むことを特徴とする方法。
【請求項２】
前記ターゲット暗号化ノードが前記第４の鍵に基づいて前記保護鍵暗号文を復号化する前に、
前記ターゲット暗号化ノードが前記鍵管理システムから送信された鍵パラメータ暗号文を受信するステップであって、鍵パラメータ暗号文は、前記鍵管理システムによって前記第３の鍵を用いて前記鍵パラメータを暗号化することにより得られる、ステップと、
前記ターゲット暗号化ノードが前記第４の鍵を用いて前記鍵パラメータ暗号文を復号化し、復号化して得られた結果が前記鍵パラメータと一致した場合、前記第４の鍵に基づいて前記保護鍵暗号文を復号化する動作を実行することを決定するステップと、をさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ターゲット暗号化ノードが第２のビデオ暗号文に対する復号化の指示を検出した場合、前記第２のビデオ暗号文から第２の鍵暗号文と第２の鍵ＩＤを抽出するステップと、
前記ターゲット暗号化ノードが前記第２の鍵ＩＤに基づいて前記鍵管理システムから第２の保護鍵を取得するステップであって、前記第２の保護鍵は、前記ターゲット暗号化ノードから送信された、前記第２の鍵ＩＤが付加される保護鍵の取得要求に応答して、前記ターゲット暗号化ノードの検証に合格した場合に、前記鍵管理システムによって前記ターゲット暗号化ノードに送信される、ステップと、
前記ターゲット暗号化ノードが前記第２の保護鍵に基づいて前記第２の鍵暗号文を復号化し、第２のビデオ鍵を得るステップと、
前記ターゲット暗号化ノードが前記第２のビデオ鍵に基づいて前記第２のビデオ暗号文を復号化するステップと、をさらに含むことを特徴とする請求項１に記載の方法。
【請求項４】
鍵管理システムと複数の暗号化ノードとを含むビデオデータスライスの暗号化システムにおけるターゲット暗号化ノードに適用されるビデオデータスライスの暗号化装置であって、前記ターゲット暗号化ノードは前記複数の暗号化ノードのいずれかであり、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライス

は、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、
　第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するための取得ユニットであって、前記第１の保護鍵は、前記ターゲット暗号化ノードの検証に合格した場合に、前記鍵管理システムによって前記ターゲット暗号化ノードに送信され、同じ鍵ＩＤに対応する保護鍵は同じである、取得ユニットと、
　第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るための暗号化ユニットであって、前記暗号化ユニットはさらに、前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るために用いられる、暗号化ユニットと、
　前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するための処理ユニットと、を含み、
　前記第１の鍵ＩＤに基づいて前記鍵管理システムから前記第１の保護鍵を取得するとき、前記取得ユニットは、
　第２の乱数を生成し、前記第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成し、
　前記ターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズムを用いて、前記ターゲット暗号化ノードのデバイスＩＤ、前記第１の鍵ＩＤ、及び前記鍵パラメータに署名し、第１の署名データを得、
　前記デバイスＩＤ、前記第１の鍵ＩＤ、前記鍵パラメータ、及び前記第１の署名データを前記鍵管理システムに送信することにより、前記鍵管理システムに、前記デバイスＩＤに基づいて前記ターゲット暗号化ノードの公開鍵を取得させ、前記ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて前記第１の署名データを検証させ、検証に合格した場合、第３の鍵に基づいて、前記第１の鍵ＩＤに対応する前記第１の保護鍵を暗号化させ、保護鍵暗号文を得させ、ここで、前記第３の鍵は、前記鍵管理システムによって、前記鍵パラメータと前記鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて生成され、
　前記鍵管理システムから送信された前記保護鍵暗号文を受信し、
　前記鍵管理システムの公開鍵と前記第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成し、
　前記第４の鍵に基づいて前記保護鍵暗号文を復号化し、前記第１の保護鍵を得るために用いられる、ことを特徴とする装置。
【請求項５】
　ビデオデータスライスの暗号化システムであって、鍵管理システムと複数の暗号化ノードを含み、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスは、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、
　前記暗号化ノードがターゲット暗号化ノードとする場合、第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得し、第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るために用いられ、同じ鍵ＩＤに対応する保護鍵は同じであり、
　前記鍵管理システムが前記ターゲット暗号化ノードの検証に合格した場合に、前記第１の鍵ＩＤに対応する前記第１の保護鍵を前記ターゲット暗号化ノードに送信するために用いられ、
　前記暗号化ノードがターゲット暗号化ノードとする場合、さらに、前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るために用いられ、
　前記暗号化ノードがターゲット暗号化ノードとする場合、さらに、前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するために用いられ、
　前記暗号化ノードがターゲット暗号化ノードとする場合、第２の乱数を生成し、前記第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラ

メータを生成し、前記ターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズムを用いて、前記ターゲット暗号化ノードのデバイスＩＤ、前記第１の鍵ＩＤ、及び前記鍵パラメータに署名し、第１の署名データを得、前記デバイスＩＤ、前記第１の鍵ＩＤ、前記鍵パラメータ、及び前記第１の署名データを前記鍵管理システムに送信するために用いられ、

前記鍵管理システムが前記ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて前記第１の署名データを検証し、検証に合格した場合、前記鍵パラメータと前記鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて第３の鍵を生成するために用いられ、

前記鍵管理システムがさらに、前記第３の鍵に基づいて、前記デバイスＩＤに対応する前記第１の保護鍵を暗号化し、保護鍵暗号文を得、前記保護鍵暗号文を前記ターゲット暗号化ノードに送信するために用いられ、

前記暗号化ノードがターゲット暗号化ノードとする場合、さらに、前記鍵管理システムから送信された前記保護鍵暗号文を受信し、前記鍵管理システムの公開鍵と前記第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成し、前記第４の鍵に基づいて前記保護鍵暗号文を復号化し、前記第１の保護鍵を得るために用いられる、ことを特徴とするシステム。

【請求項６】

前記鍵管理システムがさらに、前記第３の鍵を用いて前記鍵パラメータを暗号化し、鍵パラメータ暗号文を得、前記鍵パラメータ暗号文を前記暗号化ノードに送信するために用いられ、

前記暗号化ノードがターゲット暗号化ノードとする場合、さらに、前記鍵管理システムから送信された前記鍵パラメータ暗号文を受信し、前記第４の鍵を用いて前記鍵パラメータ暗号文を復号化し、復号化して得られた結果が前記鍵パラメータと一致した場合、前記第４の鍵に基づいて前記保護鍵暗号文を復号化するために用いられる、ことを特徴とする請求項５に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は情報安全性の技術分野に関し、特にビデオデータスライスの暗号化方法、装置、システム及び電子デバイスに関する。

【背景技術】

【０００２】

ビデオデータの安全性を向上させるために、ビデオデータの格納や伝送の際には、通常、ビデオデータの暗号化が必要となる。ビデオデータ暗号化の計算量とリソース消費量を削減するために、ビデオスライス及び暗号化技術は徐々にビデオデータ暗号化のための一般的な研究方向となっている。

【０００３】

しかし、実際には、従来のビデオスライスの暗号化技術では、同じビデオのすべてのスライスは、通常、同じ鍵を使用して暗号化及び復号化され、安全性が低いことが判明した。

【発明の概要】

【課題を解決するための手段】

【０００４】

以上のことから、本発明は、ビデオデータスライスの暗号化方法、装置、システム及び電子デバイスを提供する。

【０００５】

具体的に、本発明は、以下の技術的解決手段によって実現される。

【０００６】

本発明の実施形態の第１の態様によれば、鍵管理システムと複数の暗号化ノードとを含むビデオデータスライスの暗号化システムにおけるターゲット暗号化ノードに適用される

ビデオデータスライスの暗号化方法が提供され、前記ターゲット暗号化ノードは前記複数の暗号化ノードのいずれかであり、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスは、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、前記方法は、

前記ターゲット暗号化ノードが第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得し、前記ターゲット暗号化ノードが第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るステップであって、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じである、ステップと、

前記ターゲット暗号化ノードが前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るステップと、

前記ターゲット暗号化ノードが前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するステップと、を含む。

【０００７】

本発明の実施形態の第２の態様によれば、鍵管理システムと複数の暗号化ノードとを含むビデオデータスライスの暗号化システムにおけるターゲット暗号化ノードに適用されるビデオデータスライスの暗号化装置が提供され、前記ターゲット暗号化ノードは前記複数の暗号化ノードのいずれかであり、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスは、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、前記装置は、

第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するための取得ユニットであって、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じである、取得ユニットと、

第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るための暗号化ユニットであって、前記暗号化ユニットはさらに、前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るために用いられる、暗号化ユニットと、

前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するための処理ユニットと、を含む。

【０００８】

本発明の実施形態の第３の態様によれば、ビデオデータスライスの暗号化システムが提供され、前記システムは鍵管理システムと複数の暗号化ノードを含み、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスは、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、

前記暗号化ノードがターゲット暗号化ノードとする場合、第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得し、第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るために用いられ、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じであり、

前記鍵管理システムが前記ターゲット暗号化ノードの検証に合格した場合に、前記第１の鍵ＩＤに対応する前記第１の保護鍵を前記ターゲット暗号化ノードに送信するために用いられ、

前記暗号化ノードがターゲット暗号化ノードとする場合、さらに、前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るために用いられ、

前記暗号化ノードがターゲット暗号化ノードとする場合、さらに、前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するために用いられる。

【０００９】

本発明の実施形態の第４の態様によれば、鍵管理システムと複数の暗号化ノードとを含むビデオデータスライスの暗号化システムにおけるターゲット暗号化ノードに適用される電子デバイスが提供され、前記ターゲット暗号化ノードは前記複数の暗号化ノードのいず

れかであり、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスは、前記複数の暗号化ノードのうちの少なくとも２つに割り当てられて暗号化され、前記電子デバイスはプロセッサ及び機械読み取り可能な記憶媒体を含み、前記機械読み取り可能な記憶媒体には、機械実行可能命令が記憶され、前記プロセッサは、前記機械実行可能命令を実行することで、

第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得し、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じであり、

第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得、

前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得、

前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納する動作を実施するように構成される。

【発明の効果】

【００１０】

本発明の実施例に係るビデオデータスライスの暗号化方法は、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスを、少なくとも２つの暗号化ノードに割り当てて暗号化処理を行い、少なくとも２つの暗号化ノードによって同一のビデオストリーム又はビデオファイルの異なるビデオデータスライスを暗号化することにより、分散暗号化を実現し、ビデオデータスライスの暗号化効率を向上させる。また、ビデオデータスライスを暗号化する際、暗号化ノードは生成された乱数をビデオ鍵とし、鍵管理システムから取得した保護鍵を用いてビデオ鍵を暗号化することができ、これによりビデオ鍵の安全性を確保し、ビデオデータスライスの安全性を向上させる。

【図面の簡単な説明】

【００１１】

【図１】本発明の一実施形態におけるビデオデータスライスの暗号化方法のフローチャートである。

【図２】本発明の一実施形態における、ターゲット暗号化ノードが第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するフローチャートである。

【図３】本発明の一実施形態におけるビデオデータスライスの復号化方法のフローチャートである。

【図４】本発明の一実施形態におけるビデオデータスライスの暗号化方法の具体的な応用シーンのアーキテクチャ概略図である。

【図５】本発明の一実施形態におけるビデオデータスライスの暗号化方法の第１段階～第４段階のフローチャートである。

【図６】本発明の一実施形態におけるビデオデータスライスの暗号化装置の構造概略図である。

【図７】本発明の別の実施形態における別のビデオデータスライスの暗号化装置の構造概略図である。

【図８】本発明の一実施形態における電子デバイスのハードウェアの構造概略図である。

【図９】本発明の一実施形態におけるビデオデータスライスの暗号化システムの構造概略図である。

【発明を実施するための形態】

【００１２】

ここで、例示的な実施形態について詳細に説明し、その例は図面に示す。以下の説明が図面に関連する場合、特に示されない限り、異なる図面における同じ数字は、同じまたは類似の要素を表す。以下の例示的な実施形態に記載される実施形態は、本発明と一致する全ての実施形態を表すものではない。むしろ、それらは、添付の特許請求の範囲に詳細に記載された、本発明のいくつかの態様と一致する装置及び方法の例に過ぎない。

【００１３】

本発明で使用される用語は、本発明を限定するものではなく、特定の実施形態を説明するためのものである。本発明の実施形態及び添付の特許請求の範囲において使用される単数形の「１つ」、「前記」及び「当該」は、文脈が他の意味を明確に示さない限り、複数形を含むことを意図している。

【００１４】

当業者が本発明の実施形態によって提供される技術的解決策をよりよく理解し、また、本発明の実施形態の上記目的、特徴、及び利点をより明白かつ理解しやすくするために、本発明の実施形態における技術的解決策を図面と併せて以下にさらに詳細に説明する。

【００１５】

図１は、本発明の一実施形態によって提供されるビデオデータスライスの暗号化方法のフローチャートである。図１に示すように、ビデオデータスライスの暗号化方法のフローは、ステップＳ１００～ステップＳ１３０を含んでもよい。

【００１６】

本発明の実施形態では、ビデオデータスライスの暗号化の効率及び安全性を向上させるために、ビデオデータスライスの暗号化システムは、複数の暗号化ノードを含んでもよく、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスを、該当複数の暗号化ノードのうちの少なくとも２つに割り当てて暗号化処理を行ってもよい。

【００１７】

例示的に、当該少なくとも２つの暗号化ノードが、割り当てられた異なるビデオデータスライスを暗号化するときに使用する鍵（ビデオ暗号化鍵（Ｖｉｄｅｏ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ、ＶＥＫと略称する）又はビデオ鍵と呼ばれることができる）は異なる。

【００１８】

本発明の実施形態では、ビデオデータスライスの安全性をさらに向上させるために、各暗号化ノードがビデオデータスライスを暗号化するときに使用するＶＥＫを暗号化して格納してもよく、ＶＥＫを暗号化するための鍵（ビデオ鍵暗号化鍵（Ｖｉｄｅｏ　Ｋｅｙ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ、ＶＫＥＫと略称する）又は保護鍵と呼ばれることができる）は、ビデオデータスライスの暗号化システムにおける鍵管理システムによって保守してもよい。

【００１９】

例示的に、ステップＳ１００～ステップＳ１３０の実行主体は、上記複数の暗号化ノードのいずれか（本明細書では、ターゲット暗号化ノードと呼ぶ）であってもよい。

【００２０】

なお、本発明の実施形態における各ステップの番号の大きさは、実行順序の前後を意味するものではなく、各プロセスの実行順序は、本発明の実施形態の実施過程の限定を構成することなく、その機能や固有の論理によって決定されるべきである。

【００２１】

ステップＳ１００において、ターゲット暗号化ノードが第１の鍵識別子（ＩＤ）を取得し、第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得する。ここで、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じである。

【００２２】

ステップＳ１１０において、ターゲット暗号化ノードが第１の乱数を生成し、第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得る。

【００２３】

本発明の実施形態では、ターゲット暗号化ノードが割り当てられたビデオデータスライスを暗号化する必要がある場合、一方で、ターゲット暗号化ノードは１つの乱数（本明細書では第１の乱数と呼ぶ）を生成し、当該第１の乱数をビデオ鍵（本明細書では第１のビデオ鍵と呼ぶ）として、割り当てられた暗号化すべきビデオデータスライス（本明細書で

は暗号化すべきビデオデータスライスと呼ぶ）を暗号化し、対応するビデオ暗号文（本明細書では第１のビデオ暗号文と呼ぶ）を得てもよい。

【００２４】

例示的に、ビデオデータの安全性をさらに向上させるために、異なるビデオデータスライスの暗号化に使用されるビデオ鍵は異なってもよい。したがって、１つのビデオ鍵が漏洩しても、他のビデオデータスライスの安全性に影響を与えない。

【００２５】

一方、ターゲット暗号化ノードは、第１のビデオ鍵を暗号化するための保護鍵（本明細書では第１の保護鍵と呼ぶ）を鍵管理システムから取得してもよい。第１の保護鍵は、ターゲット暗号化ノードの検証に合格した場合に、鍵管理システムによってターゲット暗号化ノードに送信される。

【００２６】

例示的に、保護鍵について、鍵管理システムは、鍵ＩＤと保護鍵との間のマッピング関係の形で保守してもよく、すなわち、鍵管理システムは鍵ＩＤと保護鍵との間のマッピング関係を保守してもよい。暗号化ノードは、鍵ＩＤに基づいて、鍵管理システムから当該鍵ＩＤに対応する保護鍵を取得してもよい。

【００２７】

例示的に、鍵ＩＤと保護鍵との間のマッピング関係は１対１のマッピングであってもよく、すなわち、同じ鍵ＩＤが同じ保護鍵に対応し、異なる鍵ＩＤは異なる保護鍵に対応する。

【００２８】

一例では、ターゲット暗号化ノードは、第１の保護鍵を取得するための鍵ＩＤ（本明細書では第１の鍵ＩＤと呼ぶ）を生成してもよい。

【００２９】

例えば、ターゲット暗号化ノードは、タイムスタンプに基づいて第１の鍵ＩＤを生成してもよい。

【００３０】

例示的に、鍵管理システムは、ターゲット暗号ノードから送信された、第１の鍵ＩＤが付加される保護鍵の取得要求（第１の保護鍵取得要求と呼ぶことができ）を受信したとき、第１の保護鍵と第１の鍵ＩＤとの間のマッピング関係を決定して記録してもよい。

【００３１】

例示的に、鍵管理システムは、一定数の保護鍵を予め生成し、第１の保護鍵取得要求を受信したときに、当該一定数の保護鍵から１つの未使用の保護鍵を第１の保護鍵として選択し、第１の保護鍵と第１の鍵ＩＤとの間のマッピング関係を記録してもよい。

【００３２】

あるいは、鍵管理システムは、第１の保護鍵取得要求を受信したときに、第１の保護鍵を生成し、第１の保護鍵と第１の鍵ＩＤとの間のマッピング関係を記録してもよい。

【００３３】

別の例では、ターゲット暗号化ノードは、第１の保護鍵を取得する必要がある場合、まず鍵管理システムから第１の鍵ＩＤを取得し、その後、第１の鍵ＩＤに基づいて鍵管理システムから第１の保護鍵を取得する。

【００３４】

ステップＳ１２０において、ターゲット暗号化ノードが第１の保護鍵を用いて第１のビデオ鍵を暗号化し、第１の鍵暗号文を得る。

【００３５】

ステップＳ１３０において、ターゲット暗号化ノードが第１の鍵暗号文と第１の鍵ＩＤを第１のビデオ暗号文に格納する。

【００３６】

本発明の実施形態では、上記方法で第１の保護鍵を取得し、第１のビデオ鍵を用いて暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得た場合、第１のビ

デオ鍵の安全性を向上させるために、ターゲット暗号化ノードは、第１の保護鍵を用いて第１のビデオ鍵を暗号化し、対応する鍵暗号文（本明細書では第１の鍵暗号文と呼ぶ）を得てもよい。

【００３７】

第１のビデオ鍵を暗号化して第１の鍵暗号文を得る場合、ターゲット暗号化ノードは、第１の鍵暗号文と第１の鍵ＩＤを第１のビデオ暗号文に格納してもよい。これにより、正当なノードは、第１のビデオ暗号文中の第１の鍵ＩＤに基づいて鍵管理サーバから第１の保護鍵を取得し、当該第１の保護鍵に基づいて第１の鍵暗号文を復号化して第１のビデオ鍵を得ることができ、さらに、当該第１のビデオ鍵に基づいて第１のビデオ暗号文を復号化し、第１のビデオデータスライスを得ることができる。

【００３８】

例示的に、上記正当なノードは、上記複数の暗号化ノードのいずれか１つ、又はビデオデータ取得権限を有する他のノードを含んでもよい。

【００３９】

例示的に、ターゲット暗号化ノードは、第１の鍵暗号文と第１の鍵ＩＤを連結する（ｃｏｎｃａｔｅｎａｔｅ）方式で第１のビデオ暗号文に格納してもよく、すなわち、第１の鍵暗号文と第１の鍵ＩＤを第１のビデオ暗号文に連結してもよい。

【００４０】

このように、図１に示す方法のフローでは、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスを、少なくとも２つの暗号化ノードに割り当てて暗号化され、少なくとも２つの暗号化ノードによって同一のビデオストリーム又はビデオファイルの異なるビデオデータスライスを暗号化することにより、分散暗号化を実現し、ビデオデータスライスの暗号化効率を向上させる。また、ビデオデータスライスを暗号化する際、暗号化ノードは生成された乱数をビデオ鍵とし、鍵管理システムから取得した保護鍵を用いてビデオ鍵を暗号化することができ、これによりビデオ鍵の安全性を確保し、ビデオデータスライスの安全性を向上させる。

【００４１】

いくつかの実施形態では、図２に示すように、ステップＳ１００において、ターゲット暗号化ノードが第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するステップは、以下のステップＳ１０１～Ｓ１０６で実現され得る。

【００４２】

ステップＳ１０１において、ターゲット暗号化ノードが第２の乱数を生成し、第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成する。

【００４３】

ステップＳ１０２において、ターゲット暗号化ノードがターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズム（Ｅｌｌｉｐｔｉｃ ｃｕｒｖｅ ｃｒｙｐｔｏｇｒａｐｈｙ、ＥＣＣ）を用いて、ターゲット暗号化ノードのデバイスＩＤ、第１の鍵ＩＤ、及び鍵パラメータに署名し、第１の署名データを得る。

【００４４】

ステップＳ１０３において、ターゲット暗号化ノードがデバイスＩＤ、第１の鍵ＩＤ、鍵パラメータ、及び第１の署名データを鍵管理システムに送信することにより、鍵管理システムに、当該デバイスＩＤに基づいてターゲット暗号化ノードの公開鍵を取得させ、ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて第１の署名データを検証させ、検証に合格した場合、第３の鍵に基づいて、第１の鍵ＩＤに対応する第１の保護鍵を暗号化させ、保護鍵暗号文を得させる。当該第３の鍵は、当該鍵パラメータと鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて鍵管理システムによって生成される。

【００４５】

ステップＳ１０４において、ターゲット暗号化ノードが鍵管理システムから送信された

保護鍵暗号文を受信する。

【００４６】

ステップＳ１０５において、ターゲット暗号化ノードが鍵管理システムの公開鍵と第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成する。

【００４７】

ステップＳ１０６において、ターゲット暗号化ノードが第４の鍵に基づいて保護鍵暗号文を復号化し、第１の保護鍵を得る。

【００４８】

例示的に、保護鍵の安全性を向上させ、さらにビデオデータスライスの安全性を向上させるために、鍵管理システムから保護鍵を取得する際に、非対称アルゴリズムに基づいて取得側のデバイスを検証してもよい。

【００４９】

例示的に、第１の保護鍵を取得する必要がある場合、ターゲット暗号化ノードは、１つの乱数（本明細書では第２の乱数と呼ぶ）を生成し、当該第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成してもよい。楕円曲線については、例えば、楕円曲線デジタル署名アルゴリズム（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ、ＥＣＤＳＡ）で一般的に使用される曲線を選択してもよく、本発明の実施形態では、楕円曲線の選択について特に制限だれない。楕円曲線が決定されると、その基点も決定される。

【００５０】

例えば、第２の乱数をｒとし、楕円曲線上の基点をＧとすると、鍵パラメータＲは、以下のように生成することができる：

$$R = G \cdot r$$

ここで、「・」は楕円曲線ドット積を表す。

【００５１】

例示的に、ターゲット暗号化ノードは、上記方法で鍵パラメータを生成した場合、ターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズムを用いて、ターゲット暗号化ノードのデバイスＩＤ、第１の鍵ＩＤ、及び生成された鍵パラメータに署名し、対応する署名データ（本明細書では第１の署名データと呼ぶ）を得てもよい。

【００５２】

ターゲット暗号化ノードは、当該デバイスＩＤ、第１の鍵ＩＤ、鍵パラメータ、及び第１の署名データを鍵管理システムに送信してもよい。

【００５３】

鍵管理システムは、ターゲット暗号化ノードから送信された当該デバイスＩＤ、第１の鍵ＩＤ、鍵パラメータ、及び第１の署名データを取得すると、一方では、当該デバイスＩＤに基づいてターゲット暗号化ノードの公開鍵を照会してもよい。

【００５４】

一例として、ビデオデータスライスの暗号化システムにおける各暗号化ノードは、ビデオデータスライスを暗号化する前に、鍵管理システムに登録してもよい。登録プロセスにおいて、身元認証が完了すると、鍵管理システムは暗号化ノードの公開鍵を格納し、暗号化ノードは鍵管理システムの公開鍵を格納してもよい。

【００５５】

例示的に、鍵管理システムがターゲット暗号化ノードの公開鍵を照会した場合、ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて第１の署名データを検証してもよい。

【００５６】

一方、鍵管理システムは、受信した鍵パラメータと鍵管理システムの秘密鍵とに基づいて、楕円曲線ドット積アルゴリズムを用いて対応する鍵（本明細書では第３の鍵と呼ぶ）を生成してもよい。

【００５７】

例えば、鍵パラメータをＲとし、鍵管理システムの秘密鍵をｓとすると、第３の鍵ｋは、以下のように生成することができる：

ｋ＝Ｒ・ｓ

【００５８】

鍵管理システムが第１の署名データの検証に合格した場合、ターゲットの暗号化ノードが正当なノードであると判断することができ、このとき、鍵管理システムは、第３の鍵を用いて、第１の鍵ＩＤに対応する保護鍵（例えば、上記第１の保護鍵）を暗号化して保護鍵暗号文を得、当該保護鍵暗号文をターゲット暗号化ノードに送信してもよい。

【００５９】

例示的に、ターゲット暗号化ノードは保護鍵暗号文を受信した場合、鍵管理システムの公開鍵と第２の乱数に基づいて楕円曲線ドット積アルゴリズムを用いて対応する鍵（本明細書では第４の鍵と呼ぶ）を生成してもよい。

【００６０】

例えば、第２の乱数をｒとし、鍵管理システムの公開鍵をＳとすると、第４の鍵ｋ’は、以下のように生成することができる：

ｋ’＝Ｓ・ｒ

【００６１】

なお、ターゲット暗号ノードと鍵管理システムが共に正当なデバイスである場合、ｋとｋ’の値は同じである。

【００６２】

ターゲット暗号化ノードが第４の鍵を生成した場合、当該第４の鍵を用いて受信した保護鍵暗号文を復号化し、第１の保護鍵を得てもよい。

【００６３】

一例では、ステップＳ１０６（すなわち、ターゲット暗号化ノードが第４の鍵に基づいて保護鍵暗号文を復号化する）の前に、

ターゲット暗号化ノードが鍵管理システムから送信された鍵パラメータ暗号文を受信するステップであって、鍵パラメータ暗号文は、鍵管理システムによって第３の鍵を用いて鍵パラメータを暗号化することにより得られる、ステップと、

ターゲット暗号化ノードが第４の鍵を用いて鍵パラメータ暗号文を復号化し、復号化して得られた結果が鍵パラメータと一致した場合、第４の鍵に基づいて保護鍵暗号文を復号化する動作を実行することを決定するステップと、をさらに含んでもよい。

【００６４】

例示的に、保護鍵の信頼性を向上させ、さらにビデオデータスライスの安全性を向上させるために、鍵管理システムは保護鍵暗号文をターゲット暗号化ノードに送信する前に、第３の鍵を用いて受信した鍵パラメータを暗号化して鍵パラメータ暗号文を得、当該鍵パラメータ暗号文と上記方法で得た保護鍵暗号文をターゲット暗号化ノードに送信してもよい。

【００６５】

ターゲット暗号化ノードは、鍵パラメータ暗号文と保護鍵暗号文を受信した場合、第４の鍵を用いて鍵パラメータ暗号文を復号化し、復号化して得られた結果を上記鍵パラメータと比較し、両者が一致する場合、鍵パラメータ暗号文と保護鍵暗号文が鍵管理システムから送信されたと判断し、このとき、ターゲット暗号化ノードは第４の鍵を用いて保護鍵暗号文を復号化し、第１の保護鍵を得てもよい。

【００６６】

なお、ターゲット暗号化ノードが鍵パラメータ暗号文を受信しない場合、又は第４の鍵に基づいて受信した鍵パラメータ暗号文の復号化に失敗した場合、又は復号化して得られた結果が上記鍵パラメータと一致しない場合、受信した保護鍵暗号文は信頼できないと判断してもよく、この場合、ターゲット暗号化ノードは保護鍵暗号文を復号化する必要がない。

【００６７】

いくつかの実施形態では、図３に示すように、本発明の実施形態によって提供されるビデオデータスライスの暗号化方法は、以下のステップＳ３００～ステップＳ３３０をさらに含んでもよい。

【００６８】

ステップＳ３００において、ターゲット暗号化ノードが第２のビデオ暗号文に対する復号化の指示を検出した場合、第２のビデオ暗号文から第２の鍵暗号文と第２の鍵ＩＤを抽出する。

【００６９】

ステップＳ３１０において、ターゲット暗号化ノードが第２の鍵ＩＤに基づいて鍵管理システムから第２の保護鍵を取得する。ここで、第２の保護鍵は、ターゲット暗号化ノードの検証に合格した場合に、鍵管理システムによってターゲット暗号化ノードに送信される。

【００７０】

ステップＳ３２０において、ターゲット暗号化ノードが第２の保護鍵に基づいて第２の鍵暗号文を復号化し、第２のビデオ鍵を得る。

【００７１】

ステップＳ３３０において、ターゲット暗号化ノードが第２のビデオ鍵に基づいて第２のビデオ暗号文を復号化する。

【００７２】

例示的に、第２のビデオ暗号文は、上記第１のビデオ暗号文であってもよく、あるいは、第２のビデオ暗号文は、上記第１のビデオ暗号文以外の、本発明の実施形態によって提供されるビデオデータスライスの暗号化方法に従って暗号化された任意の他のビデオ暗号文であってもよい。

【００７３】

例示的に、ターゲット暗号化ノードが第２のビデオ暗号文に対する復号化の指示を検出した場合、ターゲット暗号化ノードは、第２のビデオ暗号文から当該第２のビデオ暗号文に格納された鍵暗号文（本明細書では、第２の鍵暗号文と呼ぶ）と鍵ＩＤ（本明細書では、第２の鍵ＩＤと呼ぶ）を抽出してもよい。

【００７４】

なお、第２のビデオ暗号文が上記第１のビデオ暗号文である場合、第２の鍵暗号文は上記第１の鍵暗号文であり、第２の鍵ＩＤは上記第１の鍵ＩＤである。

【００７５】

例示的に、ターゲット暗号化ノードは、抽出して得られた第２の鍵ＩＤに基づいて鍵管理システムから対応する保護鍵（本明細書では第２の保護鍵と呼ぶ）を取得してもよい。

【００７６】

例示的に、ターゲット暗号化ノードが第２の鍵ＩＤに基づいて鍵管理システムから第２の保護鍵を取得する具体的な実現は、上記実施形態で説明した、ターゲット暗号化ノードが第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得することに関連する実現を参照することができ、本発明の実施形態では繰り返さない。

【００７７】

ターゲット暗号化ノードは、取得した第２の保護鍵に基づいて第２のビデオ暗号文から抽出された第２の鍵暗号文を復号化し、対応するビデオ鍵（本明細書では第２のビデオ鍵と呼ぶ）を得、第２のビデオ鍵に基づいて第２のビデオ暗号文を復号化してもよい。

【００７８】

当業者が本発明の実施形態によって提供される技術的解決策をよりよく理解するために、本発明の実施形態によって提供される技術的解決策について、具体的な応用シーンに関連して以下に説明する。

【００７９】

図４を参照すると、本発明の実施形態によって提供されるビデオデータスライスの暗号化方法の具体的な応用シーンのアーキテクチャ概略図であり、図４に示すように、ビデオ

データスライスの暗号化システムは、複数の暗号化ノード（例えば、図４における暗号化ノード１～暗号化ノードＮ、Ｎは２以上の正の整数）と鍵管理システム（Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ、ＫＭＳ）を含んでもよい。鍵管理システムは、ＶＫＥＫを外部に提供してもよく、具体的には、鍵管理システムは、ＶＫＥＫの生成、配布、破棄などを担当してもよい。いくつかの実施形態では、鍵管理システムは、上記鍵管理サーバを含んでもよい。

【００８０】

図４に示すように、ビデオデータの安全性を向上させるために、ビデオデータ（ビデオストリーム又はビデオファイル）をスライスして複数のビデオデータスライス（例えば、図４のＵ１～Ｕ５）を得、当該複数のビデオデータスライスを各暗号化ノードにプッシュしてもよく、各暗号化ノードは、作業鍵（例えば、上記ビデオ鍵）をランダムに生成し、ＫＭＳと対話することによってＶＫＥＫ（例えば、上記保護鍵）を取得し、取得したＶＫＥＫを使用して作業鍵を暗号化して作業鍵暗号文（例えば、上記鍵暗号文）を取得し、生成した作業鍵を用いてビデオデータスライスを暗号化してビデオ暗号文（例えば、図４のＥＵ１～ＥＵ５）を取得し、ＶＫＥＫに対応する鍵ＩＤ及び作業鍵暗号文をビデオ暗号文に連結してもよい。

【００８１】

本実施形態において、ビデオデータスライスの暗号化方式は、登録段階、鍵要求段階、ビデオ暗号化段階、ビデオ復号化段階を含んでもよく、各段階の実現フローを以下に説明する。

【００８２】

第１段階、登録段階

【００８３】

１．１では、暗号化ノードは本ノードの公開鍵（Ｄと仮定する）とデバイスＩＤをＫＭＳに送信し、ＫＭＳは暗号化ノードの検証に合格した後、当該暗号化ノードの公開鍵Ｄとデバイスを関連付けて格納する。

【００８４】

例示的に、暗号化ノードの公開鍵は、証明書に付加されてＫＭＳに送信し、ＫＭＳによって当該証明書に基づいて暗号化ノードを検証してもよい。ＫＭＳが暗号化ノードの検証に合格した場合、ＫＭＳは証明書から暗号化ノードの公開鍵を抽出し、当該暗号化ノードのデバイスＩＤと関連付けて格納してもよい。

【００８５】

１．２では、ＫＭＳは、ＫＭＳの公開鍵（Ｓと仮定する）を暗号化ノードに送信し、暗号化ノードはＫＭＳの公開鍵を格納する。

【００８６】

例示的に、ＫＭＳの公開鍵は、証明書に付加されて暗号化ノードに送信し、暗号化ノードによって当該証明書に基づいてＫＭＳを検証してもよい。暗号化ノードがＫＭＳの検証に合格した場合、暗号化ノードは証明書からＫＭＳの公開鍵を抽出し、当該公開鍵を格納してもよい。

【００８７】

第２段階、鍵要求段階

【００８８】

２．１では、暗号化ノードはランダムにｒを生成し、楕円曲線ドット積アルゴリズムを用いてＲ＝Ｇ・ｒを計算し、鍵パラメータＲを得る。例示的に、Ｇは楕円曲線上の基点である。

【００８９】

２．２では、暗号化ノードは、ＥＣＣアルゴリズムを用いて、暗号化ノードの秘密鍵に基づいて、暗号化ノードのデバイスＩＤ、鍵ＩＤ（暗号化ノードによって生成されてもよく、例えば、タイムスタンプに基づいて生成されてもよい）、及び鍵パラメータＲに署名し、署名データＳｉｇ（デバイスＩＤ｜｜鍵ＩＤ｜｜Ｒ）（例えば、上記第１の署名デー

タ）を得る。
【００９０】
例として、「｜｜」は文字列の連結を示す。
【００９１】
２．３では、暗号化ノードは、デバイスＩＤ｜｜鍵ＩＤ｜｜Ｒ｜｜Ｓｉｇ（デバイスＩＤ｜｜鍵ＩＤ｜｜Ｒ）をＫＭＳに送信する。
【００９２】
２．４では、ＫＭＳは、デバイスＩＤに応じて暗号化ノードの公開鍵を照会し、当該公開鍵に基づいてＥＣＣアルゴリズムを用いてＳｉｇ（デバイスＩＤ｜｜ＫｅｙＩＤ｜｜Ｒ）を検証する。検証に合格した場合、２．５を実行し、合格しない場合はエラーを返す。
【００９３】
２．５では、ＫＭＳは、ＫＭＳの秘密鍵（ｓと仮定する）と鍵パラメータに基づいて、楕円曲線ドット積アルゴリズムを用いてｋ＝Ｒ・ｓを計算し、対応する鍵ｋ（例えば上記第３の鍵）を得る。
【００９４】
２．６では、ＫＭＳは、鍵ＩＤに基づき、当該鍵ＩＤに対応するＶＫＥＫ（ｖと仮定する）を照会する。
【００９５】
２．７では、ＫＭＳは、ｋを対称鍵としてＲとｖをそれぞれ暗号化し、対応する暗号文ｃ２（例えば、上記鍵パラメータ暗号文）とｃ１（例えば、上記保護鍵暗号文）を得る。
【００９６】
２．８では、ＫＭＳはｃ１とｃ２を暗号化ノードに送信する。
【００９７】
２．９では、暗号化ノードは、ＫＭＳの公開鍵Ｓと上記乱数ｒに基づき、楕円曲線ドット積アルゴリズムを用いてｋ’＝Ｓ・ｒを計算し、対応する鍵ｋ’（例えば、上記第４の鍵）を得る。
【００９８】
２．１０では、暗号化ノードはｋ’を用いてｃ２を復号化し、復号化して得られた結果がＲであれば２．１１を実行し、そうでなければエラーを返す。
【００９９】
２．１１では、暗号化ノードはｋ’を用いてｃ１を復号化し、保護鍵ｖを取得する。
【０１００】
第３段階、ビデオ暗号化段階
【０１０１】
３．１では、割り当てられたビデオデータスライスのいずれかに対する暗号化の指示が検出された場合、暗号化ノードはタイムスタンプに基づいて鍵ＩＤを生成し、当該鍵ＩＤに基づいてＫＭＳから保護鍵ｖを取得してもよい。その実施プロセスについては、上記鍵要求段階の説明を参照されたい。
【０１０２】
３．２では、暗号化ノードは乱数ｖｅｋ（例えば上記第１の乱数）を生成し、ｖｅｋを作業鍵（すなわちビデオ鍵）とする。
【０１０３】
３．３では、暗号化ノードはｖｅｋを用いて当該ビデオデータスライスを暗号化し、ビデオ暗号文を得る。
【０１０４】
３．４では、暗号化ノードはｖを用いてｖｅｋを暗号化し、ｖｅｋ暗号文（例えば上記鍵暗号文）を得る。
【０１０５】
３．５では、暗号化ノードはｖｅｋ暗号文と鍵ＩＤをビデオ暗号文に連結する。
【０１０６】

第４段階、ビデオ復号化段階

【０１０７】

４．１では、任意のビデオ暗号文（例えば上記ビデオ暗号化段階で得たビデオ暗号文）に対する復号化の指示が検出されると、暗号化ノードは当該ビデオ暗号文に付加されるｖｅｋ暗号文と鍵ＩＤを抽出する。

【０１０８】

４．２では、暗号化ノードは、鍵ＩＤに基づいてＫＭＳから保護鍵ｖを取得する。その実施プロセスについては、上記鍵要求段階の説明を参照されたい。

【０１０９】

４．３では、暗号化ノードはｖを用いてｖｅｋ暗号文を復号化し、ｖｅｋを得る。

【０１１０】

４．４では、暗号化ノードはｖｅｋを用いてビデオ暗号文を復号化する。

【０１１１】

例示的に、上記第１段階～第４段階のフローチャートを図５に示す。

【０１１２】

以上、本発明によって提供される方法について説明した。以下、本発明によって提供される装置及びシステムを説明する。

【０１１３】

図６を参照すると、図６は、本発明の一実施形態により提供されるビデオデータスライスの暗号化装置の構造概略図である。当該ビデオデータスライスの暗号化装置は、上記実施形態における暗号化ノードに適用されてもよく、図６に示すように、当該ビデオデータスライスの暗号化装置は、取得ユニット６１０と、暗号化ユニット６２０と、処理ユニット６３０とを含んでもよい。

【０１１４】

取得ユニット６１０は、第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得するために用いられる。ここで、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じである。

【０１１５】

暗号化ユニット６２０は、第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るために用いられる。

【０１１６】

前記暗号化ユニット６２０はさらに、前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るために用いられる。

【０１１７】

処理ユニット６３０は、前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するために用いられる。

【０１１８】

いくつかの実施形態において、前記取得ユニット６１０が、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得することは、

第２の乱数を生成し、前記第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成することと、

前記ターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズムを用いて、前記ターゲット暗号化ノードのデバイスＩＤ、前記第１の鍵ＩＤ、及び前記鍵パラメータに署名し、第１の署名データを得ることと、

前記デバイスＩＤ、前記第１の鍵ＩＤ、前記鍵パラメータ、及び前記第１の署名データを前記鍵管理システムに送信することにより、前記鍵管理システムに、前記デバイスＩＤに基づいて前記ターゲット暗号化ノードの公開鍵を取得させ、前記ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて前記第１の署名データを検証させ、検証に合格した場合、第３の鍵に基づいて、前記第１の鍵ＩＤに対応する前記第１

の保護鍵を暗号化させ、保護鍵暗号文を得させることであって、前記第３の鍵は、前記鍵管理システムによって、前記鍵パラメータと前記鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて生成される、ことと、
前記鍵管理システムから送信された前記保護鍵暗号文を受信することと、
前記鍵管理システムの公開鍵と前記第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成することと、
前記第４の鍵に基づいて前記保護鍵暗号文を復号化し、前記第１の保護鍵を得ることと、を含む。

【０１１９】

いくつかの実施形態において、第４の鍵に基づいて前記保護鍵暗号文を復号化する前に、前記取得ユニット６１０はさらに、
前記鍵管理システムから送信された鍵パラメータ暗号文を受信し、前記鍵パラメータ暗号文は、前記鍵管理システムによって前記第３の鍵を用いて前記鍵パラメータを暗号化することにより得られ、
前記第４の鍵を用いて前記鍵パラメータ暗号文を復号化し、復号化して得られた結果が前記鍵パラメータと一致した場合、前記第４の鍵に基づいて前記保護鍵暗号文を復号化する動作を実行することを決定するために用いられる。

【０１２０】

いくつかの実施形態において、図７を参照し、前記装置はさらに、抽出ユニット６４０と復号化ユニット６５０とを含み、
抽出ユニット６４０は、第２のビデオ暗号文に対する復号化の指示を検出した場合、前記第２のビデオ暗号文から第２の鍵暗号文と第２の鍵ＩＤを抽出するために用いられ、
前記取得ユニット６１０はさらに、前記第２の鍵ＩＤに基づいて前記鍵管理システムから第２の保護鍵を取得するために用いられ、前記第２の保護鍵は、前記ターゲット暗号化ノードの検証に合格した場合に、前記鍵管理システムによって前記ターゲット暗号化ノードに送信され、
復号化ユニット６５０は、前記第２の保護鍵に基づいて前記第２の鍵暗号文を復号化し、第２のビデオ鍵を得るために用いられ、
前記復号化ユニット６５０はさらに、前記第２のビデオ鍵に基づいて前記第２のビデオ暗号文を復号化するために用いられる。

【０１２１】

図８を参照し、図８は、本発明の実施形態によって提供される電子デバイスのハードウェアの構造概略図である。当該電子デバイスは、プロセッサ８０１及び機械読み取り可能な記憶媒体８０２を含み、前記機械読み取り可能な記憶媒体８０２には、機械実行可能命令が記憶される。プロセッサ８０１及び機械可読記憶媒体８０２は、システムバス８０３を介して通信してもよい。そして、機械読み取り可能な記憶媒体８０２のビデオデータスライスの暗号化制御ロジックに対応する機械実行可能命令を読み出して実行することで、プロセッサ８０１は、上記ビデオデータスライスの暗号化方法を実行することができる。

【０１２２】

本明細書で言及される機械読み取り可能な記憶媒体８０２は、任意の電子、磁性、光学又は他の物理的記憶装置であってもよく、実行可能なコマンド、データ等の情報を含むか又は記憶することができる。例えば、機械読み取り可能な記憶媒体は、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ、ランダムアクセスメモリ）、揮発性メモリ、不揮発性メモリ、フラッシュメモリ、記憶ドライブ（例えばハードディスクドライブ）、ソリッドステートドライブ、任意のタイプの記憶ディスク（例えば光ディスク、ｄｖｄ等）、又は類似の記憶媒体、又はそれらの組み合わせであってもよい。

【０１２３】

いくつかの実施形態では、機械読み取り可能な記憶媒体を提供し、当該機械読み取り可能な記憶媒体には、機械実行可能命令が記憶され、機械実行可能命令がプロセッサによって実行されると、上記ビデオデータスライスの暗号化方法を実施する。例えば、前記機械

読み取り可能な記憶媒体は、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、テープ、フロッピーディスク、光データ記憶装置などであってもよい。

【０１２４】

図９を参照すると、図９は、本発明の実施形態によって提供されるビデオデータスライスの暗号化システムの構造概略図である。図９に示すように、当該ビデオデータスライスの暗号化システムは、鍵管理システム９１０と複数の暗号化ノード９２０を含み、同一のビデオストリーム又はビデオファイルをスライスして得られた複数のビデオデータスライスが、前記複数の暗号化ノード９２０のうちの少なくとも２つに割り当てられて暗号化され、

前記暗号化ノード９２０がターゲット暗号化ノードとする場合、第１の鍵ＩＤを取得し、前記第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得し、第１の乱数を生成し、前記第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得るために用いられ、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じであり、

前記鍵管理システム９１０が前記ターゲット暗号化ノードの検証に合格した場合に、前記第１の鍵ＩＤに対応する前記第１の保護鍵を前記ターゲット暗号化ノードに送信するために用いられ、

前記暗号化ノード９２０がターゲット暗号化ノードとする場合、さらに、前記第１の保護鍵を用いて前記第１のビデオ鍵を暗号化し、第１の鍵暗号文を得るために用いられ、

前記暗号化ノード９２０がターゲット暗号化ノードとする場合、さらに、前記第１の鍵暗号文と前記第１の鍵ＩＤを前記第１のビデオ暗号文に格納するために用いられる。

【０１２５】

いくつかの実施形態において、前記暗号化ノード９２０がターゲット暗号化ノードとする場合、具体的に、第２の乱数を生成し、前記第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成し、前記ターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線暗号アルゴリズムを用いて、前記ターゲット暗号化ノードのデバイスＩＤ、前記第１の鍵ＩＤ、及び前記鍵パラメータに署名し、第１の署名データを得、前記デバイスＩＤ、前記第１の鍵ＩＤ、前記鍵パラメータ、及び前記第１の署名データを前記鍵管理システムに送信するために用いられ、

前記鍵管理システム９１０が、具体的に、前記ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線暗号アルゴリズムを用いて前記第１の署名データを検証し、検証に合格した場合、前記鍵パラメータと前記鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて第３の鍵を生成するために用いられ、

前記鍵管理システム９１０がさらに、具体的に、前記第３の鍵に基づいて、前記第１の鍵ＩＤに対応する前記第１の保護鍵を暗号化し、保護鍵暗号文を得、前記保護鍵暗号文を前記ターゲット暗号化ノードに送信するために用いられ、

前記暗号化ノード９２０がターゲット暗号化ノードとする場合、さらに、前記鍵管理システムから送信された前記保護鍵暗号文を受信し、前記鍵管理システムの公開鍵と前記第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成し、前記第４の鍵に基づいて前記保護鍵暗号文を復号化し、前記第１の保護鍵を得るために用いられる。

【０１２６】

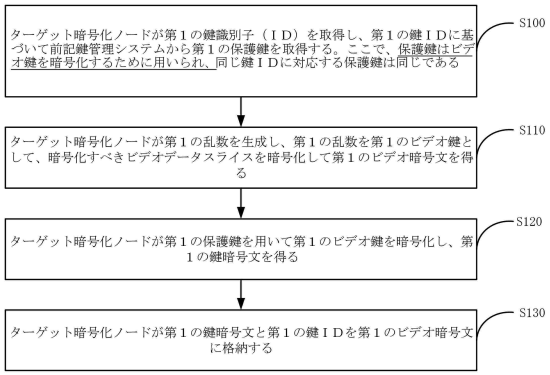
いくつかの実施形態において、前記鍵管理システム９１０がさらに、前記第３の鍵を用いて前記鍵パラメータを暗号化し、鍵パラメータ暗号文を得、前記鍵パラメータ暗号文を前記暗号化ノードに送信するために用いられ、

前記暗号化ノード９２０がターゲット暗号化ノードとする場合、前記暗号化ノード９２０がさらに、前記鍵管理システムから送信された鍵パラメータ暗号文を受信し、前記第４の鍵を用いて前記鍵パラメータ暗号文を復号化し、復号化して得られた結果が前記鍵パラメータと一致した場合、前記第４の鍵に基づいて前記保護鍵暗号文を復号化するために用いられる。

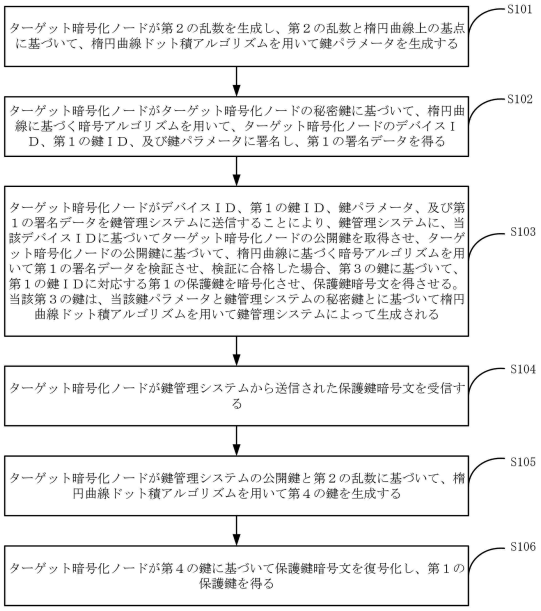
【０１２７】
なお、本明細書において、第１及び第２のような関係用語は、あるエンティティ又は動作を別のエンティティ又は動作から区別するためにのみ使用され、それらのエンティティ又は動作の間にそのような実際の関係又は順序が存在することを必ずしも要求又は示唆するものではない。さらに、「含む」、「からなる」、又はその他の変形という用語は、非排他的な包含を意図している。それにより、一連の要素を含むプロセス、方法、物品又はデバイスは、それらの要素だけでなく、明示的に列挙されていない他の要素、又はそのようなプロセス、方法、物品又は装置に固有の要素も含む。それ以上の制限がない場合、ある要素が「．．．を含む」という表現で限定された要素は、当該要素を含むプロセス、方法、物品又はデバイスに別の同じ要素の存在を排除するものではない。
【０１２８】
以上は、本発明の実施例に過ぎず、本発明を限定するものではない。当業者にとって、本発明は様々な変更及び変更が可能である。本発明の精神と原理の範囲内で行われたいかなる修正、同等置換、改善などは、本発明の請求項請求の範囲に含まれるべきである。
【符号の説明】
【０１２９】
６１０　取得ユニット
６２０　暗号化ユニット
６３０　処理ユニット
６４０　抽出ユニット
６５０　復号化ユニット
８０１　プロセッサ
８０２　機械読み取り可能な記憶媒体
８０３　システムバス
９１０　鍵管理システム
９２０　暗号化ノード

【図面】

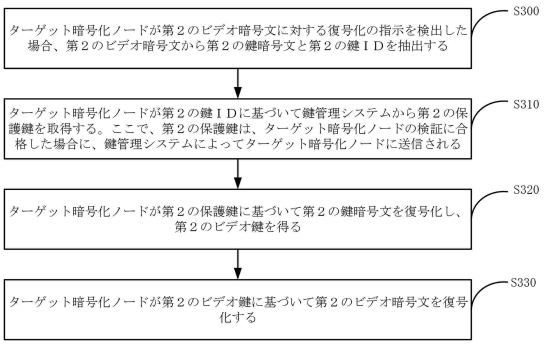
【図１】


ターゲット暗号化ノードが第１の鍵識別子（ＩＤ）を取得し、第１の鍵ＩＤに基づいて前記鍵管理システムから第１の保護鍵を取得する。ここで、保護鍵はビデオ鍵を暗号化するために用いられ、同じ鍵ＩＤに対応する保護鍵は同じである
S100
ターゲット暗号化ノードが第１の乱数を生成し、第１の乱数を第１のビデオ鍵として、暗号化すべきビデオデータスライスを暗号化して第１のビデオ暗号文を得る
S110
ターゲット暗号化ノードが第１の保護鍵を用いて第１のビデオ鍵を暗号化し、第１の鍵暗号文を得る
S120
ターゲット暗号化ノードが第１の鍵暗号文と第１の鍵ＩＤを第１のビデオ暗号文に格納する
S130

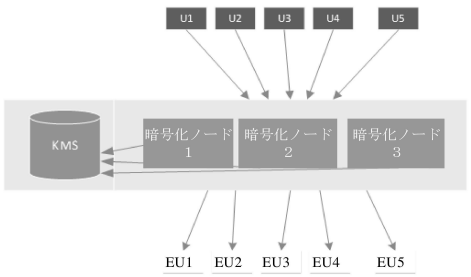
【図２】


ターゲット暗号化ノードが第２の乱数を生成し、第２の乱数と楕円曲線上の基点に基づいて、楕円曲線ドット積アルゴリズムを用いて鍵パラメータを生成する
S101
ターゲット暗号化ノードがターゲット暗号化ノードの秘密鍵に基づいて、楕円曲線に基づく暗号アルゴリズムを用いて、ターゲット暗号化ノードのデバイスＩＤ、第１の鍵ＩＤ、及び鍵パラメータに署名し、第１の署名データを得る
S102
ターゲット暗号化ノードがデバイスＩＤ、第１の鍵ＩＤ、鍵パラメータ、及び第１の署名データを鍵管理システムに送信することにより、鍵管理システムに、当該デバイスＩＤに基づいてターゲット暗号化ノードの公開鍵を取得させ、ターゲット暗号化ノードの公開鍵に基づいて、楕円曲線に基づく暗号アルゴリズムを用いて第１の署名データを検証させ、検証に合格した場合、第３の鍵に基づいて、第１の鍵ＩＤに対応する第１の保護鍵を暗号化させ、保護鍵暗号文を得させる。当該第３の鍵は、当該鍵パラメータと鍵管理システムの秘密鍵とに基づいて楕円曲線ドット積アルゴリズムを用いて鍵管理システムによって生成される
S103
ターゲット暗号化ノードが鍵管理システムから送信された保護鍵暗号文を受信する
S104
ターゲット暗号化ノードが鍵管理システムの公開鍵と第２の乱数に基づいて、楕円曲線ドット積アルゴリズムを用いて第４の鍵を生成する
S105
ターゲット暗号化ノードが第４の鍵に基づいて保護鍵暗号文を復号化し、第１の保護鍵を得る
S106

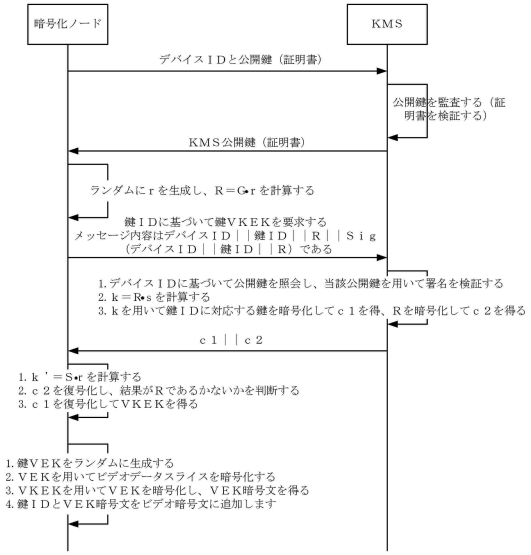
【図３】


ターゲット暗号化ノードが第２のビデオ暗号文に対する復号化の指示を検出した場合、第２のビデオ暗号文から第２の鍵暗号文と第２の鍵ＩＤを抽出する
S300
ターゲット暗号化ノードが第２の鍵ＩＤに基づいて鍵管理システムから第２の保護鍵を取得する。ここで、第２の保護鍵は、ターゲット暗号化ノードの検証に合格した場合に、鍵管理システムによってターゲット暗号化ノードに送信される
S310
ターゲット暗号化ノードが第２の保護鍵に基づいて第２の鍵暗号文を復号化し、第２のビデオ鍵を得る
S320
ターゲット暗号化ノードが第２のビデオ鍵に基づいて第２のビデオ暗号文を復号化する
S330

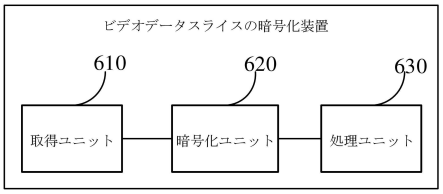
【図４】


U1
U2
U3
U4
U5
KMS
暗号化ノード1
暗号化ノード2
暗号化ノード3
EU1
EU2
EU3
EU4
EU5

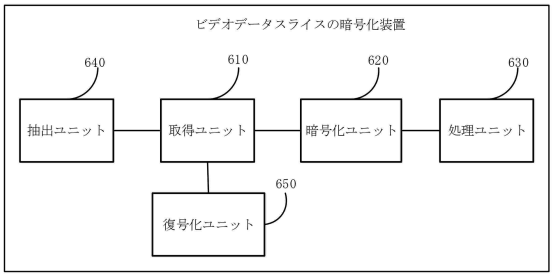
【図５】


暗号化ノード
KMS
デバイスＩＤと公開鍵（証明書）
公開鍵を監査する（証明書を検証する）
KMS公開鍵（証明書）
ランダムにｒを生成し、Ｒ＝Ｇ•ｒを計算する
鍵ＩＤに基づいて鍵ＶＫＥＫを要求する
メッセージ内容はデバイスＩＤ｜｜鍵ＩＤ｜｜Ｒ｜｜Ｓｉｇ
（デバイスＩＤ｜｜鍵ＩＤ｜｜Ｒ）である
1. デバイスＩＤに基づいて公開鍵を照会し、当該公開鍵を用いて署名を検証する
2. ｋ＝Ｒ•ｓを計算する
3. ｋを用いて鍵ＩＤに対応する鍵を暗号化してｃ１を得、Ｒを暗号化してｃ２を得る
ｃ１｜｜ｃ２
1. ｋ＇＝Ｓ•ｒを計算する
2. ｃ２を復号化し、結果がＲであるかないかを判断する
3. ｃ１を復号化してＶＫＥＫを得る
1. 鍵ＶＥＫをランダムに生成する
2. ＶＥＫを用いてビデオデータスライスを暗号化する
3. ＶＫＥＫを用いてＶＥＫを暗号化し、ＶＥＫ暗号文を得る
4. 鍵ＩＤとＶＥＫ暗号文をビデオ暗号文に追加します

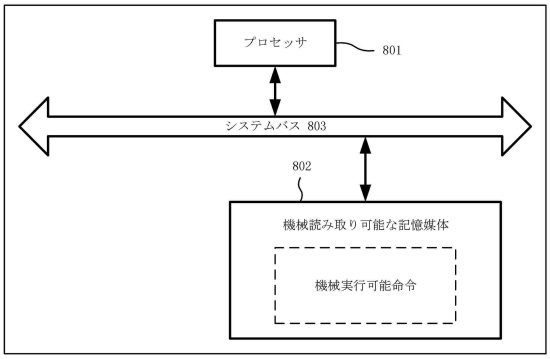
【図６】


ビデオデータスライスの暗号化装置
610
620
630
取得ユニット
暗号化ユニット
処理ユニット

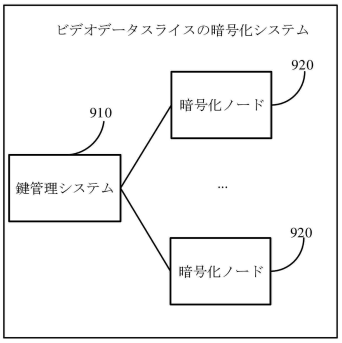
【図７】


ビデオデータスライスの暗号化装置
640
610
620
630
抽出ユニット
取得ユニット
暗号化ユニット
処理ユニット
650
復号化ユニット

【図８】


プロセッサ
801
システムバス 803
802
機械読み取り可能な記憶媒体
機械実行可能命令

【図９】



フロントページの続き

(72)発明者　▲陳▼ 加▲棟▼
中華人民共和国３１００５１浙江省杭州市▲濱▼江区阡陌路５５５号
(72)発明者　姚 相振
中華人民共和国３１００５１浙江省杭州市▲濱▼江区阡陌路５５５号
(72)発明者　李 琳
中華人民共和国３１００５１浙江省杭州市▲濱▼江区阡陌路５５５号
(72)発明者　黄 晶晶
中華人民共和国３１００５１浙江省杭州市▲濱▼江区阡陌路５５５号

審査官　平井 誠
(56)参考文献　中国特許出願公開第１０６２３１３４６（ＣＮ，Ａ）
特開２００５－２８４５２５（ＪＰ，Ａ）
特開２００２－１７６４１９（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／００－４０
Ｇ０６Ｆ　２１／００－８８