(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7481076号
(P7481076)

(45)発行日　令和6年5月10日(2024.5.10)

(24)登録日　令和6年4月30日(2024.4.30)

(51)国際特許分類

		FI		
G06F 21/60 (2013.01)		G06F	21/60	360
G09C 1/00 (2006.01)		G09C	1/00	660D
G06F 3/06 (2006.01)		G06F	3/06	301W
		G06F	21/60	320

請求項の数　20　（全23頁）

(21)出願番号　特願2022-504000(P2022-504000)
(86)(22)出願日　令和2年7月31日(2020.7.31)
(65)公表番号　特表2022-544009(P2022-544009A)
(43)公表日　令和4年10月17日(2022.10.17)
(86)国際出願番号　PCT/IB2020/057249
(87)国際公開番号　WO2021/028771
(87)国際公開日　令和3年2月18日(2021.2.18)
審査請求日　令和4年12月23日(2022.12.23)
(31)優先権主張番号　16/540,088
(32)優先日　令和1年8月14日(2019.8.14)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MACHINES CORPORATION
アメリカ合衆国１０５０４ ニューヨーク州 アーモンク ニュー オーチャード ロード
New Orchard Road, Armonk, New York 10504, United States of America
(74)代理人　100112690
弁理士　太佐 種一

最終頁に続く

(54)【発明の名称】　キー圧縮可能な暗号化

(57)【特許請求の範囲】

【請求項１】

プロセッサと、前記プロセッサによってアクセス可能なメモリと、前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と、前記メモリに格納され、前記プロセッサによってアクセス可能なデータとを含む、コンピュータ・システムに実装される方法であって、

前記コンピュータ・システムで、元のデータ・セクタを圧縮して、新しいデータ・セクタの部分を生成すること；

前記コンピュータ・システムで、前記新しいデータ・セクタの部分を、データ暗号化キー（ＤＥＫ）を用いて暗号化すること；

前記コンピュータ・システムで、前記圧縮された前記新しいデータ・セクタの部分に、メタデータおよびパディング・データを付加すること；

前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに

前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること

を含む方法。

【請求項２】

圧縮されている前記元のデータ・セクタが所定量未満に圧縮されている場合に、前記元のデータ・セクタを圧縮しないこと；

前記コンピュータ・システムで、データ暗号キー（ＤＥＫ）を用いて前記未圧縮の元のデータ・セクタを暗号化すること；および
前記コンピュータ・システムで、前記暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送すること
をさらに含む、請求項１に記載の方法。
【請求項３】
プロセッサと、前記プロセッサによってアクセス可能なメモリと、前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と、前記メモリに格納され、前記プロセッサによってアクセス可能なデータとを含む、コンピュータ・システムに実装される方法であって、
前記コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること；
圧縮されている前記元のデータ・セクタが所定量未満に圧縮されている場合に、前記元のデータ・セクタを圧縮しないこと；
前記コンピュータ・システムで、データ暗号キー（ＤＥＫ）を用いて前記未圧縮の元のデータ・セクタを暗号化すること；ならびに
前記コンピュータ・システムで、前記暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送すること
を含み、
前記ストレージ・システムは、前記ＤＲＫを用いて前記コンピュータ・システムから送信された前記データ・セクタのうち少なくとも一部を復号し、圧縮可能なパターンの有無を用いて、前記伝送されたデータが圧縮されているか否かを判定し；
前記データ・セクタが圧縮されていないと判定された際に、次いで、前記ストレージ・システムは、修正することなく前記未圧縮の元のデータ・セクタを格納し；
前記データ・セクタが圧縮されていると判定された際に、次いで、前記ストレージ・システムは、前記ＤＲＫを用いてホストによって送信された前記データ・セクタを復号し、前記復号された新しいデータ・セクタを格納し；
前記ストレージ・システムが圧縮能を内蔵している際に、前記ストレージ・システムは、前記圧縮可能なパターンを利用して格納スペースを節約する、
方法。
【請求項４】
プロセッサと、前記プロセッサによってアクセス可能なメモリと、前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と、前記メモリに格納され、前記プロセッサによってアクセス可能なデータとを含む、コンピュータ・システムに実装される方法であって、
前記コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること；
前記コンピュータ・システムで、前記ストレージ・システムから暗号化されたデータ・

セクタを受信すること；
前記コンピュータ・システムで、前記ＤＲＫを用いて、前記暗号化されたデータ・セクタのうち少なくとも１つのデータ・セクタを復号すること；
前記コンピュータ・システムで、前記復号されたデータ・セクタのうち少なくとも一部分におけるパディング・データの存在に基づき、前記データ・セクタが圧縮データを含むか否かを判定すること；
前記データ・セクタが圧縮されている際に、前記コンピュータ・システムで、前記ＤＥＫを用いて前記圧縮データを復号すること、および前記コンピュータ・システムで、前記復号された圧縮データを解凍すること；ならびに
前記データ・セクタが圧縮されていない際に、前記コンピュータ・システムで、前記ＤＥＫを用いて、前記暗号化されたデータ・セクタを解凍することなく復号すること；
を含み、
前記メタデータは、前記元のデータ・セクタの圧縮長の値を含み、前記値は、前記ＤＲＫを用いて前記圧縮データを復号した後に、前記圧縮データを解凍するために使用される、方法。
【請求項５】
プロセッサと、前記プロセッサによってアクセス可能なメモリと、前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と、前記メモリに格納され、前記プロセッサによってアクセス可能なデータとを含む、コンピュータ・システムに実装される方法であって、
前記コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
を含み、
前記ストレージ・システムは、
前記ストレージ・システムで、格納されたデータ・がパディング・データを含むか否かを判定すること；
前記格納されたデータ・セクタがパディング・データを含む際に、前記ストレージ・システムで、前記ＤＲＫを用いて前記格納されたデータ・セクタを暗号化して、暗号化されたデータ・セクタを形成し、前記暗号化されたデータ・セクタを前記コンピュータ・システムに伝送すること；ならびに
前記格納されたデータ・セクタがパディング・データを含まない際に、前記格納されたデータ・セクタを前記暗号化されたデータ・セクタとして前記コンピュータ・システムに伝送すること
によって、暗号化されたデータ・セクタを伝送する、方法。
【請求項６】
プロセッサと、前記プロセッサによってアクセス可能なメモリと、前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と、前記メモリに格納され、前記プロセッサによってアクセス可能なデータとを含む、コンピュータ・システムに実装される方法であって、
前記コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデー

タ・セクタを暗号化すること；
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること；ならびに
重複排除をサポートするストレージ・システムに前記データ・セクタが伝送される際に、前記コンピュータ・システムで、同一データの異なるデータ・セクタについて同一の初期化ベクトルが生成され、前記ＤＥＫによる今後の復号のための前記メタデータの一部として前記初期化ベクトルを追加するように；ならびに
前記データ・セクタが圧縮可能ではない際に、次いで、セクタ番号に基づき初期化ベクトルを生成するように、
前記ＤＥＫおよび初期化ベクトルを用いてデータを暗号化することを含む、方法。
【請求項７】
前記ＤＥＫを用いた前記復号が、前記メタデータに含まれる前記初期化ベクトルを用いて実施される、請求項６に記載の方法。
【請求項８】
プロセッサと；前記プロセッサによってアクセス可能なメモリと；前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と；前記メモリに格納され、
元のデータ・セクタを圧縮して、新しいデータ・セクタの部分を生成すること；
前記新しいデータ・セクタの部分を、データ暗号化キー（ＤＥＫ）を用いて暗号化すること；
前記圧縮された前記新しいデータ・セクタの部分に、メタデータおよびパディング・データを付加すること；
データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに
前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
を行うように前記プロセッサによってアクセス可能なデータと
を含むシステム。
【請求項９】
圧縮されている前記元のデータ・セクタが所定量未満に圧縮されている場合に、前記元のデータ・セクタを圧縮しないこと；
データ暗号キー（ＤＥＫ）を用いて前記未圧縮の元のデータ・セクタを暗号化すること；および
前記暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送することをさらに含む、請求項８に記載のシステム。
【請求項１０】
プロセッサと；前記プロセッサによってアクセス可能なメモリと；前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と；前記メモリに格納され、
メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること、
圧縮されている前記元のデータ・セクタが所定量未満に圧縮されている場合に、前記元のデータ・セクタを圧縮しないこと；
データ暗号キー（ＤＥＫ）を用いて前記未圧縮の元のデータ・セクタを暗号化すること；ならびに
前記暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送すること
を行うように前記プロセッサによってアクセス可能なデータと
を含み、

前記ストレージ・システムは、前記ＤＲＫを用いて前記コンピュータ・システムから送信された前記データ・セクタのうち少なくとも一部を復号し、圧縮可能なパターンの有無を用いて、前記伝送されたデータが圧縮されているか否かを判定し；
前記データ・セクタが圧縮されていないと判定された際に、次いで、前記ストレージ・システムは、修正することなく前記未圧縮の元のデータ・セクタを格納し；
前記データ・セクタが圧縮されていると判定された際に、次いで、前記ストレージ・システムは、前記ＤＲＫを用いてホストによって送信された前記データ・セクタを復号し、前記復号された新しいデータ・セクタを格納し；
前記ストレージ・システムが圧縮能を内蔵している際に、前記ストレージ・システムは、前記圧縮可能なパターンを利用して格納スペースを節約する、
システム。
【請求項１１】
プロセッサと；前記プロセッサによってアクセス可能なメモリと；前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と；前記メモリに格納され、
メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
前記ストレージ・システムから暗号化されたデータ・セクタを受信すること；
前記ＤＲＫを用いて、前記暗号化されたデータ・セクタのうち少なくとも１つのセクタを復号すること；
前記復号されたデータ・セクタのうち少なくとも一部分におけるパディング・データの存在に基づき、前記データ・セクタが圧縮データを含むか否かを判定すること；
前記データ・セクタが圧縮されている際に、前記コンピュータ・システムで、前記ＤＥＫを用いて前記圧縮データを復号すること、および前記コンピュータ・システムで、前記復号された圧縮データを解凍すること；ならびに
前記データ・セクタが圧縮されていない際に、前記コンピュータ・システムで、前記ＤＥＫを用いて、前記暗号化されたデータ・セクタを解凍することなく復号すること；
を行うように前記プロセッサによってアクセス可能なデータと
を含み、
前記メタデータは、前記元のデータ・セクタの圧縮長の値を含み、前記値は、前記ＤＲＫを用いて前記圧縮データを復号した後に、前記圧縮データを解凍するために使用される、
システム。
【請求項１２】
プロセッサと；前記プロセッサによってアクセス可能なメモリと；前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と；前記メモリに格納され、
メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに
前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
を行うように前記プロセッサによってアクセス可能なデータと
を含み、
前記ストレージ・システムは、
前記ストレージ・システムで、格納されたデータ・セクタがパディング・データを含むか否かを判定すること；

前記格納されたデータ・セクタがパディング・データを含む際に、前記ストレージ・システムで、前記ＤＲＫを用いて前記格納されたデータ・セクタを暗号化して、暗号化されたデータ・セクタを形成し、前記暗号化されたデータ・セクタを前記コンピュータ・システムに伝送すること；ならびに
前記格納されたデータ・セクタがパディング・データを含まない際に、前記格納されたデータ・セクタを前記暗号化されたデータ・セクタとして前記コンピュータ・システムに伝送すること
によって、暗号化されたデータ・セクタを伝送する、システム。
【請求項１３】
プロセッサと；前記プロセッサによってアクセス可能なメモリと；前記メモリに格納され、前記プロセッサによって実行可能なコンピュータ・プログラム命令と；前記メモリに格納され、
メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに
前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
を行うように前記プロセッサによってアクセス可能なデータと
を含み、
重複排除をサポートするストレージ・システムに前記データ・セクタが伝送される際に、前記コンピュータ・システムで、同一データの異なるデータ・セクタについて同一の初期化ベクトルが生成され、前記ＤＥＫによる今後の復号のための前記メタデータの一部として前記初期化ベクトルを追加すること；ならびに
前記データ・セクタが圧縮可能ではない際に、次いで、セクタ番号に基づき初期化ベクトルを生成すること
によって、前記ＤＥＫおよび初期化ベクトルを用いてデータを暗号化することをさらに含む、システム。
【請求項１４】
前記ＤＥＫを用いた前記復号が、前記メタデータに含まれる前記初期化ベクトルを用いて実施される、請求項１３に記載のシステム。
【請求項１５】
併せて具現化されるプログラム命令を有するコンピュータ・プログラムであって、前記プログラム命令は、
前記コンピュータ・システムで、元のデータ・セクタを圧縮して、新しいデータ・セクタの部分を生成すること；
前記コンピュータ・システムで、前記新しいデータ・セクタの部分を、データ暗号化キー（ＤＥＫ）を用いて暗号化すること；
前記コンピュータ・システムで、前記圧縮された前記新しいデータ・セクタの部分に、メタデータおよびパディング・データを付加すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
を含む方法を前記コンピュータ・システムに実施させるよう、コンピュータ・システムによって実行可能である、コンピュータ・プログラム。
【請求項１６】
圧縮されている前記元のデータ・セクタが所定量未満に圧縮されている場合に、前記元のデータ・セクタを圧縮しないこと；
前記コンピュータ・システムで、データ暗号キー（ＤＥＫ）を用いて前記未圧縮の元の

データ・セクタを暗号化すること；および
前記コンピュータ・システムで、前記暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送すること
をさらに含む、請求項１５に記載のコンピュータ・プログラム。
【請求項１７】
併せて具現化されるプログラム命令を有するコンピュータ・プログラムであって、前記プログラム命令は、
コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
圧縮されている前記元のデータ・セクタが所定量未満に圧縮されている場合に、前記元のデータ・セクタを圧縮しないこと；
前記コンピュータ・システムで、データ暗号キー（ＤＥＫ）を用いて前記未圧縮の元のデータ・セクタを暗号化すること；ならびに
前記コンピュータ・システムで、前記暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送すること
を含む方法を前記コンピュータ・システムに実施させるよう、コンピュータ・システムによって実行可能であり、
前記ストレージ・システムは、前記ＤＲＫを用いて前記コンピュータ・システムから送信された前記データ・セクタのうち少なくとも一部を復号し、圧縮可能なパターンの有無を用いて、前記伝送されたデータが圧縮されているか否かを判定し；
前記データ・セクタが圧縮されていないと判定された際に、次いで、前記ストレージ・システムは、修正することなく前記未圧縮の元のデータ・セクタを格納し；
前記データ・セクタが圧縮されていると判定された際に、次いで、前記ストレージ・システムは、前記ＤＲＫを用いてホストによって送信された前記データ・セクタを復号し、前記復号された新しいデータ・セクタを格納し；
前記ストレージ・システムが圧縮能を内蔵している際に、前記ストレージ・システムは、前記圧縮可能なパターンを利用して格納スペースを節約する、
コンピュータ・プログラム。
【請求項１８】
併せて具現化されるプログラム命令を有するコンピュータ・プログラムであって、前記プログラム命令は、
コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること；
前記コンピュータ・システムで、前記ストレージ・システムから暗号化されたデータ・セクタを受信すること；
前記コンピュータ・システムで、前記ＤＲＫを用いて、前記暗号化されたデータ・セクタのうち少なくとも１つのデータ・セクタを復号すること；
前記コンピュータ・システムで、前記復号されたデータ・セクタのうち少なくとも一部

分におけるパディング・データの存在に基づき、前記データ・セクタが圧縮データを含むか否かを判定すること；
前記データ・セクタが圧縮されている際に、前記コンピュータ・システムで、前記ＤＥＫを用いて前記圧縮データを復号すること、および前記コンピュータ・システムで、前記復号された圧縮データを解凍すること；ならびに
前記データ・セクタが圧縮されていない際に、前記コンピュータ・システムで、前記ＤＥＫを用いて、前記暗号化されたデータ・セクタを解凍することなく復号すること；
を含む方法を前記コンピュータ・システムに実施させるよう、コンピュータ・システムによって実行可能であり、
前記メタデータは、前記元のデータ・セクタの圧縮長の値を含み、前記値は、前記ＤＲＫを用いて前記圧縮データを復号した後に、前記圧縮データを解凍するために使用される、コンピュータ・プログラム。
【請求項１９】
併せて具現化されるプログラム命令を有するコンピュータ・プログラムであって、前記プログラム命令は、
コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；ならびに
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること
を含む方法を前記コンピュータ・システムに実施させるよう、コンピュータ・システムによって実行可能であり、
前記ストレージ・システムは、
前記ストレージ・システムで、格納されたデータ・セクタがパディング・データを含むか否かを判定すること；
前記格納されたデータ・セクタがパディング・データを含む際に、前記ストレージ・システムで、前記ＤＲＫを用いて前記格納されたデータ・セクタを暗号化して、暗号化されたデータ・セクタを形成し、前記暗号化されたデータ・セクタを前記コンピュータ・システムに伝送すること；ならびに
前記格納されたデータ・セクタがパディング・データを含まない際に、前記格納されたデータ・セクタを前記暗号化されたデータ・セクタとして前記コンピュータ・システムに伝送すること
によって、暗号化されたデータ・セクタを伝送する、コンピュータ・プログラム。
【請求項２０】
併せて具現化されるプログラム命令を有するコンピュータ・プログラムであって、前記プログラム命令は、
コンピュータ・システムで、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成することによって、前記元のデータ・セクタを圧縮すること；
前記コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、前記新しいデータ・セクタを暗号化すること；
前記コンピュータ・システムで、前記暗号化された新しいデータ・セクタをストレージ・システムに伝送すること；
重複排除をサポートするストレージ・システムに前記データ・セクタが伝送される際に、前記コンピュータ・システムで、同一データの異なるデータ・セクタについて同一の初期化ベクトルが生成され、前記ＤＥＫによる今後の復号のための前記メタデータの一部と

して前記初期化ベクトルを追加すること；ならびに
前記データ・セクタが圧縮可能ではない際に、次いで、セクタ番号に基づき初期化ベクトルを生成すること；
によって、前記ＤＥＫおよび初期化ベクトルを用いてデータを暗号化すること
を含む方法を前記コンピュータ・システムに実施させるよう、コンピュータ・システムによって実行可能であり、
前記ＤＥＫを用いた前記復号は、前記メタデータに含まれる前記初期化ベクトルを用いて実施される、
コンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はキー圧縮可能な暗号化に関する。
【背景技術】
【０００２】
多くの現代のストレージ・システムは、スペースを節約しストレージをよりよく利用するために、圧縮もしくは重複排除またはその両方技術を使用するデータ削減能に内蔵されている。このやり方により、格納されている実際の内容に応じて、ストレージのコストを大幅に削減することができる。しかし、データセンタおよびクラウドストレージにおけるやがて到来する傾向とは、ホスト側暗号化を使用すること、すなわち、データをストレージに送信する前にアプリケーション・サーバから離れたまま暗号化して、エンドツーエンド暗号化を配信することである。このようなやり方は、セキュリティ上の利益をもたらすものの、ストレージ・システムに到達するデータは既に暗号化された形式であり、もはや圧縮できない（典型的な暗号化データは圧縮または重複排除の可能性を持たない）。
【０００３】
そのため、圧縮および重複排除の利益を維持しつつ、ホスト側暗号化を提供しようとする場合に問題が生じる。従来のアプローチの１つは、暗号化される前にホスト内でデータを圧縮することである。しかし、これは新たな難題を引き起こす－すなわち、圧縮データが不定の長さであり、ストレージ上でデータ・レイアウト（例えば、ログ構造アレイおよびアドレスマップなど）を管理するために複雑なデータ構造／アルゴリズムを必要とする。これは、データ内のセクタのランダムな読み取りをサポートしたい場合に特に当てはまる。これらのマッピング構造は、圧縮支持体を内蔵しているストレージ・システムに組み込まれる機構の種類である。しかし、このような機構は、典型的には、ホスト側では利用できない。
【０００４】
従来の解決策として存在するものは、ホスト側で圧縮および暗号化を行うが、データの圧縮性／重複排除の属性に関する情報を漏洩させる。そのため、ホストとストレージとの間で通信を提供しようとして、それについて盗聴している敵対者がデータの圧縮性について殆ど知らないものとなるようにするときに、問題が生じる。データ圧縮性に関する情報は、暗号化されていないデータに関するいくつかの情報を得ようとする敵対者によって使用される可能性があった。
【０００５】
したがって、データの圧縮／重複排除に関する情報を漏洩しないホストとストレージ・システムとの間の通信を提供しつつ、圧縮および重複排除の利益を維持しながら、ホスト側暗号化を提供する技術の必要性が生じる。
【発明の概要】
【０００６】
本システムおよび方法の実施形態は、圧縮および重複排除の利益を維持し、データ圧縮性／重複排除の属性に関する情報を漏洩しないホストとストレージ・システムとの間の通信を提供しながら、ホスト側暗号化を提供するための技法を提供することができる。

【０００７】
例えば、一実施形態では、方法は、プロセッサと、プロセッサによってアクセス可能なメモリと、メモリに格納されかつプロセッサによって実行可能なコンピュータ・プログラム命令と、メモリに格納されかつプロセッサによってアクセス可能なデータとを含むコンピュータ・システムに実装されてもよく、本方法は、（１）数バイトのメタデータと圧縮可能なデータのパディング（例えばゼロのシーケンス）とを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２の部分とからなる新しいセクタを作り出すことと、（２）データ削減キー（ＤＲＫ）を用いて新しい変換済みデータ・セクタをコンピュータ・システムで暗号化した後、暗号化された新しいデータ・セクタをコンピュータ・システムでストレージ・システムに伝送することとによって、新しいデータ・セクタをコンピュータ・システムで生成することを含んでいてもよい。これらは、読出し動作時のホストでの活動であり、書込み中のセクタは十分に圧縮可能である。
【０００８】
実施形態では、元のデータ・セクタが所定量を超えて圧縮できない場合、本方法は、コンピュータ・システムで、データ暗号キー（ＤＥＫ）を用いて未圧縮の元のデータ・セクタを暗号化し、コンピュータ・システムで、暗号化された未圧縮の元のデータ・セクタをストレージ・システムに伝送することができる。これらは、読出し動作時のホストでの活動であり、書込み中のセクタは十分に圧縮可能ではない。
【０００９】
ストレージ・システムは、ＤＲＫキーを用いて、ホスト側により送信されたセクタを復号しようと試みることができる。パディング・データの有無は、伝送されたデータが圧縮されているか否かを判定するためにストレージ・システムによって使用され、もし圧縮されていれば、復号された新しいデータ・セクタを格納し、圧縮されていなければ、ホストによって送信された元のセクタに戻り、修正することなくそれを格納する。これらは、読出し動作時のストレージ・システムでの活動である。
【００１０】
ホスト側から送信されたセクタが本来圧縮可能であったか否かを判定する際に、ストレージ・システムは、ＤＲＫを用いてセクタの先頭のみを復号しようと試行することができる。セクタの先頭が圧縮可能なデータ・パターン（例えばゼロのシーケンス）を含まない場合に、次いでストレージは、セクタの残りを復号する必要はなく、さらに修正することなく格納することができる。
【００１１】
本方法は、ストレージ・システムで、要求されたセクタが圧縮可能なパディング・データのシーケンス（例えばゼロのシーケンス）を含有するか否かをチェックし、含有する場合、ＤＲＫを用いてそれを暗号化してホストに送信し、含有していない場合、それをそのままホストに送信することを含んでいてもよい。これらは、読出し動作時のストレージ・システムでの活動である。
【００１２】
本方法は、コンピュータ・システムで、ストレージ・システムからのデータのセクタを受信することと；コンピュータ・システムで、ＤＲＫを用いて、暗号化されたデータ・セクタの少なくとも一部を復号することと；コンピュータ・システムで、圧縮可能なパディング・データの有無に基づき、データ・セクタが圧縮データを含むか否かを判定することとを、さらに含んでいてもよい。セクタが圧縮されていると判定された場合、本方法は、コンピュータ・システムで、ＤＥＫを用いて圧縮データを復号し、コンピュータ・システムで、復号された圧縮データを解凍する。データ・セクタが圧縮されていないと判定された場合、本方法は、コンピュータ・システムで、暗号化されたデータ・セクタを復号する。これらは、リード動作時のホストでの動作であるこれらは、読出し動作時のホストでの活動である。
【００１３】

圧縮セクタ内のメタデータは、圧縮されている元のデータ・セクタの圧縮長を標示する値を含むことがあり、この値は、解凍アルゴリズムに用いるパラメータとしてホストが使用することができる。ストレージ・システムが重複排除をサポートする場合、本方法は、コンピュータ・システムで、ＤＥＫおよび生成された初期化ベクトルを用いてデータを暗号化することをさらに含むことがあり、この初期化ベクトルは、同一データのセクタについて同一であるセクタ・データから（例えばキー付きハッシュを用いて）生成される。

【００１４】

一実施形態では、システムは、プロセッサと；プロセッサによってアクセス可能なメモリと；メモリに格納され、プロセッサによって実行可能なコンピュータ・プログラム命令と；メモリに格納されるデータであって、元のデータ・セクタを圧縮すること、メタデータおよびパディング・データを含む第１の部分と、データ暗号化キー（ＤＥＫ）を用いて圧縮および暗号化されている元のデータ・セクタを含む第２のデータとを含む新しいデータ・セクタを生成すること、データ削減キー（ＤＲＫ）を用いて新しいデータ・セクタを暗号化すること、ならびに暗号化された新しいデータ・セクタをストレージ・システムに伝送すること、を行うようにプロセッサによってアクセス可能であるデータとを含む。

【００１５】

一実施形態では、コンピュータ・プログラム製品は、それにより具現化されるプログラム命令、すなわちコンピュータによって実行可能なプログラム命令を有する非一時的コンピュータ可読ストレージを含むことがあり、プログラム命令は、コンピュータ・システムで元のデータ・セクタを圧縮すること、データ暗号化キー（ＤＥＫ）を用いて、メタデータおよびパディング・データを含む第１の部分と、圧縮および暗号化されている元のデータ・セクタを含む第２の部分とを含む新しいデータ・セクタを生成すること、コンピュータ・システムで、データ削減キー（ＤＲＫ）を用いて、新しいデータ・セクタを暗号化すること、ならびにコンピュータ・システムで、暗号化された新しいデータ・セクタをストレージ・システムに伝送すること、を含む方法をコンピュータに実施させるものである。

【００１６】

圧縮および重複排除の利益を維持し、データの圧縮性／重複排除の属性に関する情報を漏洩しない通信を提供しながら、データの暗号化を提供するための技術について、以下に説明する。

【００１７】

本発明の詳細は、その構造と動作との両方に関して、同様の参照番号および名称が同様の要素を指す添付図面を参照することによって、最もよく理解することができる。

【図面の簡単な説明】

【００１８】

【図１】本技術の実施形態によるシステムの例示的なブロック図である。

【図２】本システムおよび方法の実施形態による、ホスト側の単一セクタの書込み動作の例示的な擬似コード図である。

【図３】本システムおよび方法の実施形態による、ストレージ側の単一セクタの書込み動作の例示的な擬似コード図である

【図４】本システムおよび方法の実施形態による、ストレージ側の単一セクタの読出し動作の例示的な擬似コード図である

【図５】本システムおよび方法の実施形態による、ホスト側の単一セクタの読出し動作の例示的な擬似コード図である

【図６】本明細書に記載の実施形態に含まれる処理を実装することができる、コンピュータ・システムの例示的なブロック図である

【発明を実施するための形態】

【００１９】

本システムおよび方法の実施形態は、データの圧縮性／重複排除の属性に関する情報を漏洩しないホストとストレージ・システムとの間の通信を提供しつつ、圧縮および重複排除の利益を維持しながら、ホスト側暗号化を提供するための技法を提供することができる

。実施形態は、「キー圧縮可能な暗号化」、すなわち、データ削減キーを保有するストレージ・システムが、データの圧縮および重複排除の利益のいくらかを得ることを可能にし得る暗号化方法を実施することができる。さらに、データ削減キーを保有しないいかなる敵対者も、データのデータ削減の属性に関する情報を全く学習しないかまたは殆ど学習しないものとなる。

【００２０】

実施形態では、ストレージ・コントローラに書き込まれた暗号化された各セクタは、その元のセクタのサイズおよびオフセットと共に書き込まれ、データ・レイアウトを担うストレージを保ち、圧縮されたブロックを管理する必要に気付かないホストを保つものとしてよい。実施形態は、データ・セクタを（もし十分に圧縮可能であれば）圧縮し、２つの部分からなる新しいセクタ（元のセクタと同じ長さを有する）を作成することができる。一方の部分は、例えば、いくつかのメタデータ・バイトと、圧縮可能なパターン（例えば、ゼロのシーケンス）とを含むことができる。第２の部分は、データ暗号キー（ＤＥＫ）を用いて暗号化された圧縮データを含んでいてもよい。最も一般的な設定では、これらの２つの部分は連結され、次いでデータ減少キー（ＤＲＫ）を用いて暗号化され、ストレージ・システムに送られる。実施形態では、ＤＥＫおよびＤＲＫは、暗号化と復号との両方に使用される対称キーとしてもよいし、他の実施形態では、非対称または異なるキーを、暗号化および復号（例えば、プライベート・キーおよび公開キー）に用いてもよい。

【００２１】

次いで、ＤＲＫを保持するストレージ・システムは、第２の暗号化層を復号してデータを格納することができる。ストレージ・システムがデータ圧縮能を有する場合、セクタを（例えば、圧縮可能なパディングを除去することによって）圧縮形態で格納してもよい。ストレージ・システムは、決してデータを明瞭に見ないものとしてよく、ＤＥＫへのアクセスを有していなくてもよいが、データ圧縮性を学習しない。盗聴者は、（圧縮されずに暗号化されているかのように）データについて何も学習しない。付加的な利益は、データ削減能を特定のストレージ・システムに結び付ける能力である。さらに、実施形態は、重複排除のサポートおよび性能の最適化を含めた数多くの最適化を含むことができる。

【００２２】

本技術の実施形態によるシステム１００の例示的なブロック図を図１に示す。この例では、システム１００は、ホスト・システム１０２、ストレージ・システム１０４、およびネットワーク１０６を含むことがある。典型的には、ホスト・システムは、ストレージ・システム１０４上にセクタ１０８などのデータを格納することができる１つまたは複数のコンピュータ・システムとしてよく、ストレージ・システム１０４からデータを読み出すものとしてよい。ホスト・システム１０２は、パーソナル・コンピュータ、ワークステーション、スマートフォン、タブレット・コンピュータ、サーバ・システムなどのような任意のタイプのコンピュータ・システムを含むことがある。同様に、ストレージ・システム１０４は、パーソナル・コンピュータ、ワークステーション、スマートフォン、タブレット・コンピュータ、サーバ・システムなどの任意のタイプのコンピュータ・システムを含むことがあるが、典型的には、大量のデータを格納するためのサーバ・システムを含む。ネットワーク１０６は、ホスト・システム１０２とストレージ・システム１０４との間の通信を提供してもよい。このような通信は、双方向性であっても直接的または間接的であってもよい。ネットワーク１０６は、ローカル・エリア・ネットワーク、広域ネットワーク、標準または専有のネットワーク、私用または公用のネットワークなどの任意の数および任意の組合せのネットワークを含み得るが、典型的にはインターネットを含んでいることがある。

【００２３】

例えば、セクタ書込み動作において、ホスト・システム１０２は、セクタ１０８にホスト書込み処理１１０を実行して、処理されたセクタをストレージ・システム１０４に送信することによって、セクタ１０８をストレージ・システム１０４に書き込むことができ、ストレージ・システム１０４は、受信された処理済みセクタへのストレージ・システム書

込み処理１１２を実施し、その結果得られたデータをセクタ１１４として記憶することができる。同様に、ホスト・システム１０２は、格納されたセクタ１１２へのストレージ・システム読出し処理１１８をストレージ・システム１０４に実施させて、処理されたセクタをホスト・システム１０２に伝送することによって、格納されたセクタ１１６をストレージ・システム１０４から読み出し、ホスト・システム１０２は、受信した処理済みセクタへのホスト・システム読出し処理１２０を実施して、結果データであるセクタ１２２を得ることができる。ホスト・システム１０２への書込み処理１１０および読出し処理１２０は、データ暗号化キー（ＤＥＫ）１２４を用いて実施されてもよく、いくつかの状況では、下記に記載されるように、データ削減キー（ＤＲＫ）１２６を用いて実施されてもよい。ストレージ・システム１０４への書込み処理１１２および読出し処理１１８は、データ削減キー（ＤＲＫ）１２６を用いて実施されてもよい。ストレージ・システム１０４は、データ暗号化キー（ＤＥＫ）１２４を使用せず、これに関する知識を持たない。システム１００の動作を、図２、図３、図４，および図５を参照して下記にさらに記載する。

【００２４】

概して、処理の実施形態は、各データ・ブロック、セクタ、またはチャンク毎にホストで行われてもよい。簡単にするために、用語セクタを本明細書に用いることができるが、用語セクタは物理的格納セクタのみを指すのではなく、むしろ任意のブロック、セクタ、チャンクまたは他の量のデータを指すことを理解されたい。データ・セクタは、ＤＥＫを用いて圧縮および暗号化されてもよい。次いで、暗号化および圧縮されたセクタ・データは、圧縮可能なパディングと連結されて、元の長さのセクタを形成してもよい。また、いくつかのメタデータをパディングの一部として付加してもよい。新しいパディングされたブロックは、次いで、ＤＲＫにより暗号化されて、ストレージに送信されてもよい。

【００２５】

本技術による、データをストレージ・システム１０４に書き込むホスト・システム・プロセス２００の例示的なフロー図を、図２に示す。図１と併せると最も良く見える。ホスト側書込みプロセス２００は２０２で開始することができ、２０２では、格納すべきデータのセクタ（またはブロックまたはチャンク）１０８を圧縮することができる。ｘを圧縮後のセクタのサイズとする。２０４では、セクタ・データ１０８がｋバイト超圧縮されていない場合に、次いで、元の未圧縮のセクタ１０８は、データ暗号化キー（ＤＥＫ）１２４を用いて暗号化されてもよく、暗号化された未圧縮のセクタは、ストレージ・システム１０４に格納のために送信されてもよい。ステップ２０６では、セクタ１０８が２０４でｋ以上のバイトで圧縮された場合に、次いで、プレフィックス（またはサフィックス、本技術をいずれかまたは両方に適用されてもよい）が作成されてもよく、このプレフィックスは、元のセクタ・サイズから圧縮後のセクタのサイズを引いたもの（ＳＥＣＴＯＲ＿ＳＩＺＥ－ｘ）に等しいサイズを有する。このプレフィックスは、メタデータ（例えば圧縮長を符号化したもの）と、圧縮可能なシーケンス、例えばゼロのシーケンスとを足し合わせて含むことができる。２０８では、サイズのプレフィックス（ＳＥＣＴＯＲ＿ＳＩＺＥ－ｘ）２１０は、ＤＥＫ２１２を用いて暗号化されているｘバイトの圧縮セクタと連結されてもよい。２１４では、連結されたデータは、データ削減キー（ＤＲＫ）１２６を用いて暗号化されてもよく、暗号化された圧縮セクタ・データは、ストレージ・システム１０４に格納のために送信されてもよい

【００２６】

暗号化方法に応じて、ＤＥＫを用いて暗号化され得るメッセージのサイズに制限がある場合がある。その場合には、値ｘは、圧縮後のセクタのサイズを、ＤＥＫを用いて暗号化できるサイズに丸めて示す。

【００２７】

なお、ストレージ・システムに送信される全てのバイトは、ホストによって暗号化されてもよい。その結果、ホストとストレージ・システムとの間の通信を盗聴する敵対者は、データの圧縮性に関する情報を得ない。

【００２８】

ストレージ・システム書込みプロセス３００は３０２で開始することができ、３０２では、ストレージ・システム１０４は、格納すべきデータを受信することができ、受信データを復号するためにＤＲＫを用いることができる。３０４では、ストレージ・システム１０４は、復号された受信データを調べることができる。プレフィックスが、十分に長い圧縮可能なシーケンス、例えばゼロのシーケンスを含まない場合、これは圧縮可能なセクタではなく、ＤＲＫ復号前の受信データ、すなわちＤＥＫ暗号化された元のセクタは、格納されてもよい１１４。あるいは、３０６で、復号された受信データが格納されてもよい。これにより、（ＳＥＣＴＯＲ＿ＳＩＺＥ－ｘ）バイトの圧縮可能なプレフィックス（暗号化されていない）３０８と、ＤＥＫ１０８を用いて暗号化されたｘバイトの圧縮セクタ３１０とを含む、格納データ１１４が得られる

【００２９】

なお、ストレージ・システムに書き込まれる暗号化されていないプレフィックスは、圧縮可能なパターン（例えばゼロのシーケンス）を含む。実施形態では、ストレージ・システムは、省スペース化につながるデータ削減能を有していてもよい。

【００３０】

さらに、実施形態は、同一のセクタ（プレーンテキスト）を同一の暗号化セクタとしてストレージ・システムに書き込むことができる、重複排除しやすい暗号化を用いてもよい。実施形態では、このストレージ・システムは、重複排除に基づくデータ削減能を有していてもよく、それにより、さらに進んだ省スペース化に至る可能性がある。

【００３１】

本技術によるストレージ・システム１０４からデータを読み出すプロセス４００の例示的なフロー図を、図４に示す。図１と併せると最も良く見える。ストレージ・システム読出しプロセス４００は４０２で開始することができ、４０２では、格納セクタ１１６がｋバイトのパディング・プレフィックスを含む場合に、次いで、セクタ１１６は、ＤＲＫ１２６を用いて暗号化されて、ホスト１０２に送信されてもよい。あるいは、４０４で、セクタ１１６がｋバイトのパディング・プレフィックスを持たない場合に、セクタ１１６は圧縮されず、セクタ１１６はそのままホスト１０２に送信される。

【００３２】

ホスト側読み取りプロセス５００は５０２で開始することができ、５０２では、ストレージ・システム１０４から受信されたデータは、ＤＲＫ１２６を用いて復号化されてもよい。５０４では、これがパディング・プレフィックスを含まない復号されたセクタを生じた場合に、ＤＥＫ暗号化されたセクタである（ＤＲＫによる復号の前の）ストレージ・システム１０４からの元の受信データは、次いで、ＤＥＫ１２４を用いて復号されてセクタ１２２を得ることができる。

【００３３】

５０６で、あるいは、復号されたセクタがパディング・プレフィックスを含まない場合、次いで、メタデータは、例えば、圧縮されたセクタのサイズを示す２バイトをプレフィックスから得ることができる。メタデータは、解凍のためのパラメータとして使用されてもよい。５０８では、ＤＥＫ１２４を用いて、圧縮セクタを復号して圧縮セクタを形成することができる。次に、５０８で、メタデータ３０８を用いて、圧縮セクタを全ＳＥＣＴＯＲ＿ＳＩＺＥバイトに解凍してセクタ（１２２）を形成することができる

【００３４】

多くの暗号化機構では、セクタ暗号化の結果は、データ、暗号化キー、および初期化ベクトル（ＩＶ）に依存し得る。ＩＶは、同一のプレーンテキスト・セクタが同じ暗号化セクタに暗号化されるのを防止するために使用されてもよい。実施形態では、ＩＶは、例えば、セクタ番号から計算することができる。

【００３５】

本システムおよび方法の実施形態は、重複排除を支援する方法で、圧縮可能なデータを暗号化してもよい。重複排除を達成するために、同一のプレーンテキスト・セクタは、ストレージ・システム上の同一の暗号化セクタにマッピングされるものとするべきである。

したがって、実施形態では、ＩＶは、セクタ番号から導出されない場合がある。代わりに、実施形態は、プレーンテキスト・データのキー付きハッシュ（例えばＤＥＫ）からＩＶを導出してもよい。例えば、実施形態は、セクタ・データに連結されたＤＥＫのＳＨＡ２５６を用いてもよい。このＩＶは、復号を可能にするために、暗号化されたセクタに追加されてもよい。このため、ホストとストレージ・システムとの間のプロトコルが変更されていない場合には、セクタ内の空きスペースを使用してＩＶデータを格納することができるため、圧縮可能なデータのみを実施してもよい。実施形態では、ＤＲＫによる暗号化により、重複排除の機会を隠すことができ、したがって、標準的なセクタベースのＩＶを用いるものとなる。

【００３６】

実施形態は、圧縮不能なセクタに対処することができる。書込み動作時に、ホストが、セクタが圧縮不能であると判定した場合に、実施形態は、セクタ番号から導出されたＩＶを用いてＤＥＫを用いる前に、セクタを暗号化することができる。この暗号化されたセクタは、ストレージ・システムに送信されてもよい。ストレージ・システムは、この暗号化されたセクタを圧縮セクタとして扱うか未圧縮セクタとして扱うかを決定することができる。未圧縮である場合には、次いで、そのまま書き込むべきとなる。圧縮されている場合には、次いで、プリフィックス・セクタは、ストレージに書き込まれる前に復号されてもよい。セクタが圧縮可能であるか否かを判定するための１つの方法は、ＤＲＫを用いて、暗号化されたセクタの開始を復号しようと試行することである。その結果が圧縮可能なパターンを含んでいれば、次いで、セクタは圧縮可能である。

【００３７】

本システムおよび方法の実施形態で実装され得る追加の特徴としては、例えば、ホストが全ての圧縮可能なセクタを１個のゼロバイトで開始させることによって、圧縮可能なセクタをマークする（これにより、ＤＲＫ暗号化されたプレフィックスのサイズを１バイト減少させる）ことができるという、性能向上を挙げることができる。ストレージは、ゼロバイトで開始しないいかなるセクタも圧縮可能ではないことを確実に知るものとなる。ストレージがゼロから始まるセクタを受信した場合には、それが圧縮可能ではない可能性があり、暗号化されたセクタが偶然にもゼロバイトで開始する。ストレージは、上述したように、ＤＲＫを用いてプレフィックスの開始を復号しようと試行することによって、最終的な決定を行うことができる。これにより、セクタが圧縮可能であるか否かについて（しかし圧縮性のレベルについてではない）いくらかの情報が漏洩することがあるが、圧縮不能なセクタに対する不要な復号の試行の数を大幅に減少させ得る。

【００３８】

さらに、セクタが圧縮可能であることを標示するために１バイトを送信するのではなく、実施形態は、複数個のゼロバイトを送信してもよい。例えば、圧縮可能なセクタが３個のゼロバイトで表示されている場合には、セクタが圧縮可能なセクタとして誤って識別されている（ＤＲＫによりそれを復号するようストレージ・システムを不必要に試行させることに繋がる）可能性は、２５６＾３における１である。

【００３９】

別の実施形態は、チャンクがＤＲＫ暗号化されているか否かを標示するメタデータと、ＤＲＫキーが使用されたことを標示するキー＿ＩＤとを含んでいてもよい。例えば、非破壊的なキー回転を可能にするために、１対のビットを異なるキーに追加してもよい。

【００４０】

実施形態では、ホストとストレージ・システムとの間のプロトコルは、例えば、セクタが圧縮可能か否かを標示する追加の単一ビットを伝えるように変更されてもよい。これにより、ＤＲＫによる圧縮不能なセクタの不要な復号を防止するものとなる。

【００４１】

実施形態は、重複排除をサポートしないストレージ・システムを含んでいてもよい。このような実施形態では、全ての暗号化は、セクタ番号から導出されたＩＶを利用することができ、すなわち、同一のプレーンテキスト・セクタを同一の暗号化されたセクタに確実

に変換するものとする必要はない。ストレージ・システムが重複排除をサポートしていない実施形態では、同一の暗号化されたセクタを同一の暗号化セクタに変換することができるため、暗号化されたデータを再び暗号化して、（同一の暗号化されたセクタを識別することによって）データの重複排除性に関する情報を盗聴者が得るのを防止することができる。したがって、重複排除をサポートしない実施形態では、ホストは、ＤＲＫによりプレフィックスのみを暗号化することができる。圧縮データは、ＤＥＫにより１回のみ暗号化されることがある（さらに別のＤＲＫ暗号化を行わない）。

【００４２】

実施形態では、ストレージは、プレフィックス全体を復号しない場合がある。それは、メタデータ・バイトおよび圧縮可能なパターン（例えば３０個のゼロバイト）を含む短いプレフィックスまたはプレフィックスの一部のみを復号することがある。圧縮可能なパターンは、データが実際に圧縮された十分な証拠として機能することがあり、メタデータから、完全な圧縮可能なパターンの長さが決定されてもよい。そのため、プレーンテキストが圧縮可能なパターンであることをストレージが既に知っている際に、暗号化された圧縮可能なパターンの残りの部分を復号する必要はないものとなる。読出しの間に、同じことをホスト側の動作にも適用することができる

【００４３】

実施形態では、ストレージ・システムは、そのデータ削減能を改善するために、ホスト側で圧縮が行われるという事実を利用してもよい。ストレージ・システムが圧縮セクタを識別する場合、次いで、圧縮可能なパターンとそれに続いて（さらに圧縮できない）暗号化された圧縮データのシーケンスとがあることを直ちに学習する。圧縮不能なデータを圧縮しようと試行するストレージ・システムには意味がない。かといって、高度な圧縮アルゴリズムを用いて、圧縮可能なパターン（例えばゼロのシーケンス）を圧縮しようと試みることにも意味がなく、圧縮可能なパターンが単に除去されるのみで格納されないこともある。読出し時に、セクタがＳＥＣＴＯＲ＿ＳＩＺＥよりも短い場合には、次いで、ストレージは、ＤＲＫにより再暗号化する前に、パディング・プレフィックスを満たすことができる。

【００４４】

実施形態は、重複排除をサポートしないストレージ・システムを含んでいてもよい。このような実施形態では、圧縮セクタのプレフィックスは、データのハッシュ（初期化ベクトル）を含むことができる。ストレージ・システムが重複排除能を有する場合には、次いで、重複排除のためにこのハッシュを利用してもよい。これにより以下の２つの利点がある：ａ）ハッシュを再計算する必要性をストレージ・システムから除くことができる、ならびにｂ）ストレージが典型的にはＤＲＫを使用してデータ部分を復号するところ、同一のセクタが既に存在していると（ハッシュに基づいて）ストレージ・システムが判断した場合には、圧縮データを復号する必要は全くない。

【００４５】

記載されたキー圧縮可能なアルゴリズムによって、圧縮可能なセクタのうち同一のセクタのシーケンスを識別するための重複排除能を有するストレージが実現する。しかし、圧縮不能なセクタのうち、または圧縮可能なセクタと圧縮不能なセクタとの混合物のうち、同一のセクタのシーケンスを識別することはできない。実施形態は、ＤＲＫを用いて暗号化される圧縮不能なセクタのハッシュを含むように、ホストとストレージ・システムとの間のプロトコルを変更することによって、この機能性を提供してもよい。これらのハッシュがストレージ・システム上で復号されると、ストレージ・システムは、全ての暗号化されたデータに対して重複排除を行うために、圧縮可能なセクタと圧縮不能なセクタとの両方のハッシュに関する情報を利用することができる。

【００４６】

本明細書に記載の実施形態に含まれるプロセスが実装され得るコンピュータ・システム５００の例示的なブロック図を、図５に示す。コンピュータ・システム５００は、内蔵プロセッサ、チップ上のシステム、パーソナル・コンピュータ、ワークステーション、サー

バ・システム、ミニコンピュータ、またはメインフレームコンピュータなどの１つまたは複数のプログラムされた汎用コンピュータ・システムを用いて、または分散型ネットワーク・コンピューティング環境で、実装されてもよい。コンピュータ・システム５００は、１つまたは複数のプロセッサ（ＣＰＵ）５０２Ａ～５０２Ｎと、入出力回路５０４と、ネットワーク・アダプタ５０６と、メモリ５０８とを含んでいてもよい。ＣＰＵ５０２Ａ～５０２Ｎは、現在の通信システムおよび方法の機能を実施するために、プログラム命令を実行する。典型的には、ＣＰＵ５０２Ａ～５０２Ｎは、ＩＮＴＥＬ　ＣＯＲＥ（登録商標）プロセッサなどの１つまたは複数のマイクロプロセッサである。図５は、コンピュータ・システム５００が単一のマルチ・プロセッサ・コンピュータ・システムとして実装される実施形態を説明し、このシステムでは、マルチ・プロセッサ５０２Ａ～５０２Ｎがメモリ５０８、入出力回路５０４、およびネットワーク・アダプタ５０６などのシステム・リソースを共有する。しかし、本発明の通信システムおよび方法はまた、コンピュータ・システム５００が、単一プロセッサ・コンピュータ・システム、マルチ・プロセッサ・コンピュータ・システム、またはそれらの混合物であり得る複数のネットワーク化されたコンピュータ・システムとして実装される、実施形態を含む。

【００４７】

入出力回路５０４は、コンピュータ・システム５００からデータを入力またはデータを出力する能力を提供する。例えば、入出力回路は、キーボード、マウス、タッチパッド、トラックボール、スキャナ、アナログ－デジタル変換器などの入力デバイス、ビデオアダプタ、モニタ、プリンタなどの出力デバイス、モデムなどの入出力デバイス、ネットワーク・アダプタ５０６、ネットワーク５１０とのインターフェース・デバイス５００を含んでいてもよい。ネットワーク５１０は、任意の公衆または専用のＬＡＮまたはＷＡＮとすることができ、そのようなものとしてはインターネットが挙げられるがそれに限定されない。

【００４８】

メモリ５０８は、コンピュータ・システム５００の機能を実施するためにＣＰＵ５０２により実行されるプログラム命令と、ＣＰＵ５０２により使用されて処理されるデータとを格納する。メモリ５０８としては、例えば、ランダム・アクセス・メモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、プログラム可能な読出し専用メモリ（ＰＲＯＭ）、電気的に消去可能なプログラム可能な読出し専用メモリ（ＥＥＰＲＯＭ）、フラッシュメモリなどの電子メモリデバイス；および磁気ディスク・ドライブ、テープ・ドライブ、光学ディスク・ドライブなどの電気機械メモリであって、インテグレーティド・ドライブ・エレクトロニクス（ＩＤＥ）インターフェースに用いられ得るもの、またはそれらの変形もしくは強化物、例えばエンハンストＩＤＥ（ＥＩＤＥ）もしくはウルトラ・ダイレクト・メモリ・アクセス（ＵＤＭＡ）など；またはスモール・コンピュータ・システム・インターフェース（ＳＣＳＩ）ベースのインターフェース、またはそれらの変形もしくは強化物、例えばファスト－ＳＣＳＩ、ワイド－ＳＣＳＩ、ファスト・アンド・ワイド－ＳＣＳＩなど；またはシリアル・アドバンスト・テクノロジー・アタッチメント（ＳＡＴＡ）、またはそれらの変形もしくは強化物；またはファイバ・チャネル・アービトレーティッド・ループ（ＦＣ－ＡＬ）インターネットを挙げることができる。

【００４９】

メモリ５０８の内容は、コンピュータ・システム５００が実施するようプログラムされる機能に依存して変化し得る。図５に示される例では、例示的なメモリの内容が、ホスト・システム５１２とストレージ・システム５１４との両方に示されている。しかし、これらのルーチンは、周知の工学的な考慮に基づき、これらのルーチンに関連するメモリ内容と併せて、１つのシステムまたはデバイスに含まれていなくてもよいが、複数のシステムまたはデバイスの間で分配され得ることを、当業者は理解するものとなる。本発明の通信システムおよび方法は、そのような配置のいずれかおよび全てを含むことができる

【００５０】

図５に示される例では、メモリ５０８は、ホスト・システム５１２のために、読出しル

ーチン５１６、書込みルーチン５１８、および格納すべきデータ５２０を含み、ストレージ・システム５１４のために、読出しルーチンｓ５２２、書込みルーチン５２４、および格納されデータ５２６、および操作システム５２８を含む。ホスト・システム読出しルーチン５１６は、上述のようなホスト・システム読出しプロセスを実装するソフトウェア・ルーチンを含んでいてもよい。ホスト・システム書込みルーチン５１８は、上述のようなホスト・システム書込みプロセスを実施するソフトウェア・ルーチンを含んでいてもよい。格納すべきデータ５２０は、上述のように、ストレージ・システムに格納されるべきホスト・システム上のデータを含んでいてもよい。ストレージ・システム読出しルーチン５２２は、上述のようなストレージ・システム読出しプロセスを実施するソフトウェア・ルーチンを含んでいてもよい。ストレージ・システム書込みルーチン５２４は、上述のようなストレージ・システム書込みプロセスを実施するソフトウェア・ルーチンを含んでいてもよい。格納されたデータ５２６は、上述したように、ストレージ・システムに格納されたホスト・システムからのデータを含んでいてもよい。オペレーティング・システム・ルーチン５２８は、システム全体の機能性を提供することができる

【００５１】

図５に示されるように、本発明の通信システムおよび方法は、マルチ・プロセッサ、マルチタスキング、マルチプロセス、もしくはマルチスレッド・コンピューティング、またはそれらの組合せを提供する１つまたは複数のシステム上での実装、ならびに単一のプロセッサ、単一のスレッド・コンピューティングのみを提供するシステム上の実装を含むことができる。マルチ・プロセッサ・コンピューティングは、１つまたは複数のプロセッサを用いてコンピューティングを実施することを含む。マルチタスキング・コンピューティングは、１つを超えるオペレーティング・システム・タスクを用いてコンピューティングを実施することを含む。タスクとは、実行中のプログラムとオペレーティング・システムにより用いられる記帳情報との組合せを参照する、オペレーティング・システム概念である。プログラムが実行されるたびに、オペレーティング・システムは、そのための新しいタスクを作成する。このタスクは、プログラムをタスク番号で識別し、それに他の記帳情報を付加する、プログラムのエンベロープのようなものである。Ｌｉｎｕｘ（登録商標）、ＵＮＩＸ（登録商標）、ＯＳ／２（登録商標）、およびＷｉｎｄｏｗｓ（登録商標）を含む数多くのオペレーティング・システムは、多くのタスクを同時にランすることができ、マルチタスキング・オペレーティング・システムと呼ばれる。マルチタスキングとは、１つを超える実行可能なものをオペレーティング・システムが同時に実行する能力である。それぞれの実行可能なものは、それ自体のアドレス空間内でランしており、このことは、これらの実行可能なものが、それらのメモリのいずれかを共有する方法を持たないことを意味する。どんなプログラムでも、システム上でランする任意の他のプログラムの実行を損なうことが不可能であるため、このことは利点を有する。しかし、このプログラムは、オペレーティング・システムによる（またはファイルシステムに格納されているファイルを読み出すことによる）ことを除いて、任意の情報を交換する術がない。いくつかのオペレーティング・システムは、用語のタスクとプロセスとを区別しているが、この２つがしばしば互換的に用いられる際に、マルチプロセス・コンピューティングは、マルチタスク・コンピューティングに類似している。

【００５２】

本発明は、任意の可能な技術的詳細レベルの統合におけるシステム、方法、もしくはコンピュータ・プログラム製品、またはそれらの組合せであり得る。コンピュータ・プログラム製品は、プロセッサに本発明の態様を行わせるためのコンピュータ可読プログラム命令をその上に有するコンピュータ可読記憶媒体（または複数の媒体）を含んでいてもよい。コンピュータ可読記憶媒体は、命令実行デバイスによって使用するための命令を保持および格納することができる有形のデバイスとすることができる。

【００５３】

コンピュータ可読記憶媒体は、以下に限定されないが、例えば、電子記憶デバイス、磁気記憶デバイス、光記憶デバイス、電磁記憶デバイス、半導体記憶デバイス、または前述

の任意の適した組合せとしてよい。コンピュータ可読記憶媒体のより具体的な例の非網羅的な一覧としては、ポータブル・コンピュータ・ディスケット、ハードディスク、ランダム・アクセス・メモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、消去可能なプログラム可能な読出し専用メモリ（ＥＰＲＯＭまたはフラッシュメモリ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ）、ポータブル・コンパクト・ディスク読出し専用メモリ（ＣＤ－ＲＯＭ）、デジタル汎用ディスク（ＤＶＤ）、メモリ・スティック、フロッピー・ディスク、機械的に符号化されたデバイス、例えば、命令を上に記録したパンチ・カードまたは溝内の隆起構造など、および前述の任意の適切な組合せが挙げられる。コンピュータ可読記憶媒体は、本明細書で使用される際に、それ自体が電波または他の自由に伝搬する電磁波、導波管または他の伝送媒体（例えば、光ファイバ・ケーブルを通る光パルス）を伝搬する電磁波、またはワイヤを介して伝送される電気信号などの一時的な信号であるものと解釈されるべきではない。

【００５４】

本明細書に記載のコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体から各演算／処理デバイスに、またはネットワーク、例えば、インターネット、ローカル・エリア・ネットワーク、広域ネットワーク、もしくは無線ネットワーク、またはそれらの組合せを介して外部コンピュータまたは外部記憶装置に、ダウンロードすることができる。ネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、もしくはエッジ・サーバ、またはそれらの組合せを含むことができる。各演算／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェースは、ネットワークからコンピュータ可読プログラム命令を受信し、各演算／処理デバイス内のコンピュータ可読記憶媒体に格納するためにコンピュータ可読プログラム命令を送る。

【００５５】

本発明の動作を実施するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ＩＳＡ）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、集積回路のための構成データ、または１つもしくは複数のプログラミング言語の任意の組み合わせで書かれたソースコードもしくはオブジェクトコードのいずれかとしてよく、プログラミング言語としては、Ｓｍａｌｌｔａｌｋ、Ｃ＋＋などのオブジェクト指向プログラミング言語と、および「Ｃ」プログラミング言語または同様のプログラミング言語などの手続き型プログラミング言語が挙げられる。コンピュータ可読プログラム命令は、ユーザのコンピュータ上で全体的に、ユーザのコンピュータ上で部分的に、スタンドアロン・ソフトウェア・パッケージとして、ユーザのコンピュータ上で部分的にかつリモート・コンピュータ上に部分的に、またはリモート・コンピュータ上で部分的にもしくはリモート・コンピュータ上で全体的に、実行してもよい。後者のシナリオでは、リモート・コンピュータが、ローカル・エリア・ネットワーク（ＬＡＮ）または広域ネットワーク（ＷＡＮ）を含めた任意のタイプのネットワークを介してユーザのコンピュータに接続されていてもよいし、または接続が、外部コンピュータに（例えば、インターネットサービスプロバイダを用いてインターネットを介して）なされていてもよい。いくつかの実施形態では、例えば、プログラム可能な論理回路、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、またはプログラム可能な論理アレイ（ＰＬＡ）を含めた電子回路は、本発明の態様を実施するために、コンピュータ可読プログラム命令の状態情報によって、コンピュータ可読プログラム命令を実行してもよい。

【００５６】

本発明の態様は、本発明の実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図もしくはブロック図またはその両方を参照して本明細書に説明される。フローチャート図もしくはブロック図またはその両方の各ブロック、ならびにフローチャート図もしくはブロック図またはその両方におけるブロックの組合せは、コンピュータ可読プログラム命令によって実装できることが理解されよう。

【００５７】

これらのコンピュータ可読プログラム命令は、汎用コンピュータ、専用コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに提供されて、コンピュータまたは他のプログラム可能なデータ処理装置のプロセッサを介して実行される命令がフローチャートもしくはブロック図またはその両方の１つまたは複数のブロックにおいて指定された機能／動作を実装する手段を生成するように、機械を生成し得る。これらのコンピュータ可読プログラム命令はまた、コンピュータ、プログラム可能なデータ処理装置、もしくは他のデバイス、またはそれらの組合せを特定の方法で機能させることのできるコンピュータ可読記憶媒体に格納されてもよく、ゆえに、命令を中に格納したコンピュータ可読記憶媒体は、フローチャートもしくはブロック図またはその両方の１つまたは複数のブロックにおいて指定された機能／動作の態様を実装する命令を含む、製品を含み得る。

【００５８】

コンピュータ可読プログラム命令はまた、コンピュータ、他のプログラム可能な装置、または他のデバイス上で実行される命令がフローチャートもしくはブロック図またはその両方の１つまたは複数のブロックにおいて指定された機能／動作を実装するように、コンピュータ、他のプログラム可能なデータ処理装置、または他のデバイス上にロードされて、一連の動作ステップをコンピュータ、他のプログラマブル装置、または他のデバイス上で実施させて、コンピュータ実装プロセスを生じる。

【００５９】

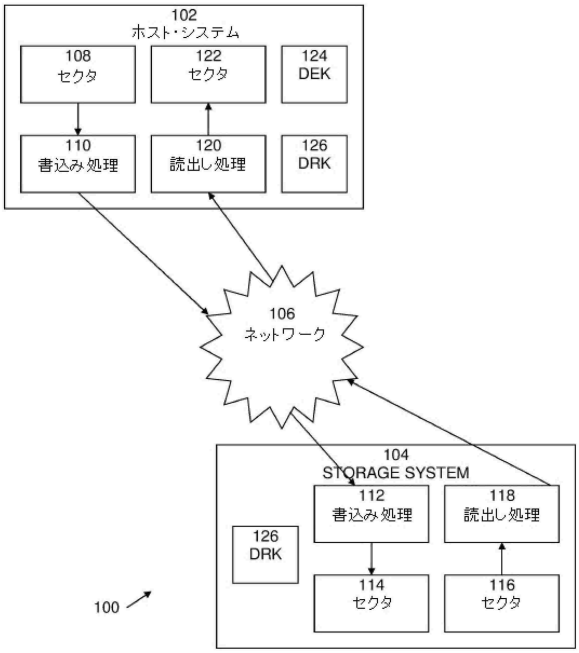
図中のフローチャートおよびブロック図は、本発明の様々な実施形態によるシステム、方法、およびコンピュータ・プログラム製品の可能な実施形態のアーキテクチャ、機能性、および動作を説明する。この点に関して、フローチャートまたはブロック図の各ブロックは、指定された論理機能を実装するための１つまたは複数の実行可能な命令を含む、命令のモジュール、セグメント、またはセクタを表すことがある。いくつかの代替的な実施形態では、ブロックに記載された機能は、図に記載された順序の外に生じ得る。例えば、連続して示される２つのブロックが、実際には、実質的に同時に実行されてもよいし、またはブロックが、関与する機能性に応じて、逆の順序で実行されてもよい。また、ブロック図もしくはフローチャート図またはその両方の各ブロック、ならびにブロック図もしくはフローチャート図またはその両方におけるブロックの組合せは、指定された機能もしくは動作を実行するか、または専用ハードウェアとコンピュータ命令との組合せを実施する、専用ハードウェアベースのシステムによって実装できることに留意されたい。

【００６０】

本発明の特定の実施形態を記載してきたが、当業者には、記載された実施形態に等しい他の実施形態が存在することが理解されよう。従って、本発明は、特定の説明された実施形態に限定されるものではなく、添付の特許請求の範囲によってのみ限定されることが理解されるべきである

【図面】

【図１】



【図２】

202：セクタを圧縮する。xを圧縮後のセクタのサイズとする。

204：データがkバイト超圧縮しない場合に、DEKにより元のデータを暗号化し、この暗号化されたセクタをストレージに送信する。

206：あるいは、サイズSECTOR_SIZE－xのプレフィックス（またはサフィックス）を作成する。このプレフィックスは、メタデータ（圧縮長を符号化したもの）とゼロのシーケンスとを足し合わせて含み得る。

208：連結：
210：（SECTOR_SIZE－x）バイトのプレフィックス
212：DEKを用いて暗号化されたxバイトの圧縮セクタ

214：DEKを用いてこの連結を暗号化する。

【図３】

302：DRKを用いてセクタを復号する。

304：プレフィックスが長いゼロのシーケンスを含まない場合に、これは圧縮可能なセクタではない。元のセクタを格納する（ＤＲＫ復号前）。

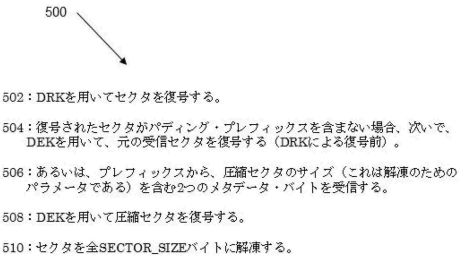
306：あるいは、結果をストレージに書き込む。この結果は、
308：（SECTOR_SIZE－x）バイトの圧縮可能なプレフィックス（暗号化されていない）
310：DEKを用いて暗号化されたxバイトの圧縮セクタ

【図４】

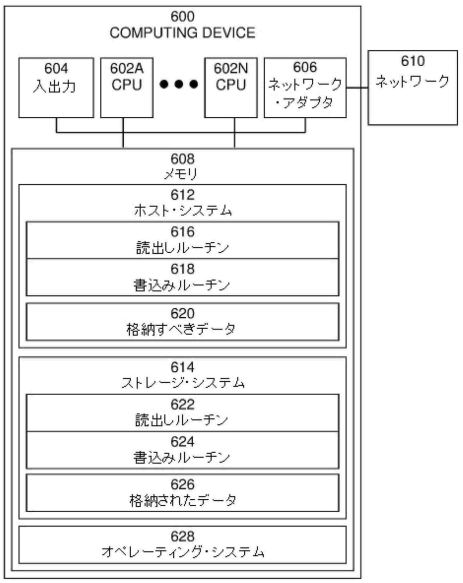
402：セクタの格納されたデータがkバイトのパディング・プレフィックスを含む場合に、次いでDRKを用いてセクタを暗号化し、ホストに送信する。

404：あるいは、全セクタをホストにそのまま送信する。

【図５】


500
502：DRKを用いてセクタを復号する。
504：復号されたセクタがパディング・プレフィックスを含まない場合、次いで、DEKを用いて、元の受信セクタを復号する（DRKによる復号前）。
506：あるいは、プレフィックスから、圧縮セクタのサイズ（これは解凍のためのパラメータである）を含む2つのメタデータ・バイトを受信する。
508：DEKを用いて圧縮セクタを復号する。
510：セクタを全SECTOR_SIZEバイトに解凍する。

【図６】


600
COMPUTING DEVICE
604
入出力
602A
CPU
602N
CPU
606
ネットワーク
・アダプタ
610
ネットワーク
608
メモリ
612
ホスト・システム
616
読出しルーチン
618
書込みルーチン
620
格納すべきデータ
614
ストレージ・システム
622
読出しルーチン
624
書込みルーチン
626
格納されたデータ
628
オペレーティング・システム

フロントページの続き

(72)発明者　チェン、ドロン
イスラエル ギバタイム、４エアリアル・シャロン・ストリート
(72)発明者　ツファディア、エリアド
イスラエル ギバタイム、４エアリアル・シャロン・ストリート
(72)発明者　ハーニク、ダニー
イスラエル ギバタイム、４エアリアル・シャロン・ストリート
(72)発明者　ファクター、マイケル
イスラエル エイチ エー３１９０５ ハイファ、マウント・カーメル、ハイファ・ユニバーシティ・キャンパス

審査官　岸野 徹

(56)参考文献
特開２０１４－０５２８９９（ＪＰ，Ａ）
特開２０１３－１０１６７２（ＪＰ，Ａ）
米国特許出願公開第２０１９／００６５７８８（ＵＳ，Ａ１）
特開２０１３－０６２６１６（ＪＰ，Ａ）
特開２０１６－１３４７５２（ＪＰ，Ａ）
米国特許出願公開第２０１６／００６２９１８（ＵＳ，Ａ１）
米国特許出願公開第２０１５／００７４４２８（ＵＳ，Ａ１）
韓国公開特許第１０－２０１５－０１２５０１０（ＫＲ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０
Ｇ０９Ｃ　１／００
Ｇ０６Ｆ　３／０６