【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成25年8月1日(2013.8.1)

【公開番号】特開2013-84294(P2013-84294A)
【公開日】平成25年5月9日(2013.5.9)
【年通号数】公開・登録公報2013-022
【出願番号】特願2012-276507(P2012-276507)
【国際特許分類】
Ｇ０６Ｆ　21/62　(2013.01)
Ｈ０４Ｌ　 9/08　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/24　１６６Ａ
Ｈ０４Ｌ　 9/00　６０１Ｂ
Ｇ０６Ｆ　21/24　１６７Ａ

【手続補正書】
【提出日】平成25年6月17日(2013.6.17)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
デジタルコンテンツを保護するセキュリティプロトコルのための方法であって、前記方法は、
第１の復号化アルゴリズムを第１のビットストリームから取得することと、
前記第１のビットストリームの残余を復号化することにより、第１の復号化されたビットストリームを生成することであって、前記第１のビットストリームの残余の復号化は、前記第１のビットストリームから取得された前記第１の復号化アルゴリズムを使用して行われる、ことと、
第２の復号化アルゴリズムを前記第１の復号化されたビットストリームから取得することと、
前記第１の復号化されたビットストリームの残余を復号化することにより、第２の復号化されたビットストリームを生成することであって、前記第１の復号化されたビットストリームの残余の復号化は、前記第１の復号化されたビットストリームから取得された前記第２の復号化アルゴリズムを使用して行われる、ことと
を含む、方法。
【請求項２】
前記第２の復号化されたビットストリームは、デジタルコンテンツを含む、請求項１に記載の方法。
【請求項３】
前記デジタルコンテンツは、オーディオデータまたはビデオデータを含む、請求項２に記載の方法。
【請求項４】
前記第１のビットストリームを第１の標的ユニットで受信することをさらに含み、前記第１のビットストリームの残余の復号化は、サーバから取得された第１のキーを使用して行われる、請求項２に記載の方法。

【請求項５】
前記第１のキーは、複合キーである、請求項４に記載の方法。
【請求項６】
前記第１のキーは、暗号化されている、請求項５に記載の方法。
【請求項７】
前記第１のキーを復号化することにより、第１の復号化された複合キーを生成することをさらに含む、請求項６に記載の方法。
【請求項８】
前記第１のキーは、標的ユニットの特定のキーを用いて復号化される、請求項７に記載の方法。
【請求項９】
前記標的ユニットの特定のキーは、前記サーバで前記標的ユニットのシリアル番号と関連付けられている、請求項８に記載の方法。
【請求項１０】
前記標的ユニットの特定のキーは、前記標的ユニットのハードウェアに常駐する、請求項９に記載の方法。
【請求項１１】
前記標的ユニットの特定のキーは、ソフトウェアによって読み取ることができない、請求項１０に記載の方法。
【請求項１２】
前記第１の復号化された複合キーを暗号化することと、前記第１の復号化されて暗号化された複合キーを局部記憶装置に格納することとをさらに含む、請求項７に記載の方法。
【請求項１３】
前記第１の復号化されたビットストリームを暗号化することと、前記第１の復号化されて暗号化されたビットストリームを局部記憶装置に格納することとをさらに含む、請求項１２に記載の方法。
【請求項１４】
前記第１の復号化された複合キーを復号化することにより、第２の復号化された複合キーを生成することをさらに含み、前記第２の復号化された複合キーは、前記第１のビットストリームの残余を復号化するために使用される、請求項７に記載の方法。
【請求項１５】
前記第２の復号化された複合キーは、ソフトウェアによって読み取ることができない、請求項１４に記載の方法。
【請求項１６】
前記第２の復号化された複合キーを暗号化することと、前記第２の復号化されて暗号化された複合キーを局部記憶装置に格納することとをさらに含む、請求項１４に記載の方法。
【請求項１７】
前記第１の復号化された複合キーは、デジタルコンテンツの特定のキーを用いて復号化される、請求項１４に記載の方法。
【請求項１８】
前記第２の復号化されたビットストリームは、キャッシュに格納される、請求項４に記載の方法。
【請求項１９】
前記キャッシュは、安全な命令キャッシュである、請求項１８に記載の方法。
【請求項２０】
デジタルコンテンツを保護するセキュリティプロトコルを実行するためのシステムであって、
前記システムは、標的ユニットを含み、前記標的ユニットは、命令を実行するように動作可能なプロセッサと、前記命令を格納するように動作可能なメモリとを含み、

前記命令は、
第１の復号化アルゴリズムを第１のビットストリームから取得するステップと、
前記第１のビットストリームの残余を復号化することにより、第１の復号化されたビットストリームを生成するステップであって、前記第１のビットストリームの残余の復号化は、前記第１のビットストリームから取得された前記第１の復号化アルゴリズムを使用して行われる、ステップと、
第２の復号化アルゴリズムを前記第１の復号化されたビットストリームから取得するステップと、
前記第１の復号化されたビットストリームの残余を復号化することにより、第２の復号化されたビットストリームを生成するステップであって、前記第１の復号化されたビットストリームの残余の復号化は、前記第１の復号化されたビットストリームから取得された前記第２の復号化アルゴリズムを使用して行われる、ステップと
を実行するように動作可能である、システム。
【請求項２１】
前記第２の復号化されたビットストリームは、デジタルコンテンツを含む、請求項２０に記載のシステム。
【請求項２２】
前記デジタルコンテンツは、オーディオデータまたはビデオデータを含む、請求項２１に記載のシステム。
【請求項２３】
前記第１のビットストリームの残余の復号化は、サーバから取得された第１のキーを使用して行われる、請求項２１に記載のシステム。
【請求項２４】
前記第１のキーは、複合キーである、請求項２３に記載のシステム。
【請求項２５】
前記第１のキーは、暗号化されている、請求項２４に記載のシステム。
【請求項２６】
前記命令は、前記第１のキーを復号化することにより、第１の復号化された複合キーを生成するステップを実行するように動作可能である、請求項２５に記載のシステム。
【請求項２７】
前記第１のキーは、標的ユニットの特定のキーを用いて復号化される、請求項２６に記載のシステム。
【請求項２８】
前記標的ユニットの特定のキーは、前記サーバで前記標的ユニットのシリアル番号と関連付けられている、請求項２７に記載のシステム。
【請求項２９】
前記標的ユニットの特定のキーは、前記標的ユニットのハードウェアに常駐する、請求項２８に記載のシステム。
【請求項３０】
前記標的ユニットの特定のキーは、ソフトウェアによって読み取ることができない、請求項２９に記載のシステム。
【請求項３１】
前記命令は、前記第１の復号化された複合キーを暗号化するステップと、前記第１の復号化されて暗号化された複合キーを局部記憶装置に格納するステップとを実行するように動作可能である、請求項２６に記載のシステム。
【請求項３２】
前記命令は、前記第１の復号化されたビットストリームを暗号化するステップと、前記第１の復号化されて暗号化されたビットストリームを局部記憶装置に格納するステップとを実行するように動作可能である、請求項３１に記載のシステム。
【請求項３３】

前記命令は、前記第１の復号化された複合キーを復号化することにより、第２の復号化された複合キーを生成するステップを実行するように動作可能であり、前記第２の復号化された複合キーは、前記第１のビットストリームの残余を復号化するために使用される、請求項２６に記載のシステム。
【請求項３４】
前記第２の復号化された複合キーは、ソフトウェアによって読み取ることができない、請求項３３に記載のシステム。
【請求項３５】
前記命令は、前記第２の復号化された複合キーを暗号化するステップと、前記第２の復号化されて暗号化された複合キーを局部記憶装置に格納するステップとを実行するように動作可能である、請求項３３に記載のシステム。
【請求項３６】
前記第１の復号化された複合キーは、デジタルコンテンツの特定のキーを用いて復号化される、請求項３３に記載のシステム。
【請求項３７】
前記第２の復号化されたビットストリームは、キャッシュに格納される、請求項２３に記載のシステム。
【請求項３８】
前記キャッシュは、安全な命令キャッシュである、請求項３７に記載のシステム。
【請求項３９】
デジタルコンテンツを保護するセキュリティプロトコルのための方法であって、前記方法は、
第１の復号化アルゴリズムを第１のビットストリームから取得することと、
前記第１のビットストリームの残余を復号化することにより、第１の復号化されたビットストリームを生成することであって、前記第１のビットストリームの残余の復号化は、前記第１のビットストリームから取得された前記第１の復号化アルゴリズムを使用して行われる、ことと、
前記第１の復号化されたビットストリームの第１の部分を取得することと、
前記第１の復号化されたビットストリームの第１の部分が、前記第１の復号化されたビットストリームの残余が暗号化されていないデジタルコンテンツであることを示すインジケータであることを決定することと
を含む、方法。
【請求項４０】
前記インジケータは、単一の演算子またはフラグである、請求項３９に記載の方法。
【請求項４１】
デジタルコンテンツを保護するセキュリティプロトコルのための方法であって、前記方法は、
第１の復号化アルゴリズムを第１のビットストリームから取得することと、
前記第１のビットストリームの残余を復号化することにより、第１の復号化されたビットストリームを生成することであって、前記第１のビットストリームの残余の復号化は、前記第１のビットストリームから取得された前記第１の復号化アルゴリズムを使用して行われる、ことと、
前記第１の復号化されたビットストリームの第１の部分を取得することと、
第２の復号化アルゴリズムを前記第１の復号化されたビットストリームの第１の部分を使用して取得することと、
前記第１の復号化されたビットストリームの残余を復号化することにより、第２の復号化されたビットストリームを生成することであって、前記第１の復号化されたビットストリームの残余の復号化は、前記第２の復号化アルゴリズムを使用して行われる、ことと
を含む、方法。
【請求項４２】

前記第１の復号化されたビットストリームの第１の部分は、メモリ内における前記第２の復号化アルゴリズムの配置である、請求項４１に記載の方法。