【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２区分
【発行日】平成22年10月28日(2010.10.28)

【公開番号】特開2010-185982(P2010-185982A)
【公開日】平成22年8月26日(2010.8.26)
【年通号数】公開・登録公報2010-034
【出願番号】特願2009-29022(P2009-29022)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６１０Ａ

【手続補正書】
【提出日】平成22年9月14日(2010.9.14)
【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】
１つの暗号鍵から拡張された、Ｎ（Ｎは２以上の自然数）個の拡張鍵を使用する暗号化装置であって、
鍵の初期値に対応するフラグを保持する第１のメモリと、
前記命令が暗号化命令でありかつ前記第１のメモリ内の前記フラグが示す鍵が前記暗号鍵である場合、前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記暗号化命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記暗号鍵を初期値として前記第２のメモリにロードする第１のセレクタと、
前記第２のメモリ内の前記暗号鍵に基づいて前記拡張鍵を計算し、当該拡張鍵を前記第１のセレクタに送る暗号化用拡張計算部を備え、
前記第１のセレクタは、初回に前記第２のメモリへ前記暗号鍵の初期値をロードし、前記暗号化命令が、前記暗号化装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記拡張鍵を前記第２のメモリにロードする、暗号化装置。
【請求項２】
前記比較結果信号に基づいて前記トリガ信号を生成するトリガ信号生成器を更に備えた、請求項１記載の暗号化装置。
【請求項３】
前記暗号化命令を発行すると共に、前記暗号鍵の初期値に対応する前記フラグを第１のメモリに設定するプロセッサを更に備えた、請求項１記載の暗号化装置。
【請求項４】
前記第１のメモリは、前記暗号鍵の初期値を保持すると共に、前記暗号鍵の初期値を前記第１のセレクタへ出力するメモリと、前記フラグを保持すると共に、前記フラグを前記比較回路へ出力するメモリとを有する、請求項１記載の暗号化装置。
【請求項５】
前記命令を発行すると共に、前記暗号鍵の初期値に対応するフラグの対を複数第３のメモリに設定するプロセッサと、

前記プロセッサが発行する鍵選択信号に基づいて前記暗号鍵の初期値に対応するフラグの対を１つ前記第１のメモリに設定する第２のセレクタを更に備えた、請求項１記載の暗号化装置。
【請求項６】
前記第２のメモリ内の前記第１の拡張鍵～前記第Ｎの拡張鍵によりデータを暗号化するＡＥＳ（Advanced Encryption Standard）方式のエンジンを更に備えた、請求項１記載の暗号化装置。
【請求項７】
１つの復号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用する復号化装置であって、
鍵の初期値に対応するフラグを保持する第１のメモリと、
前記命令が復号化命令であり、かつ、前記第１のメモリ内の前記フラグが示す鍵が前記復号鍵である場合、前記フラグ及び前記命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記復号化命令、トリガ信号及び前記比較結果信号に基づいて前記第１のメモリ内の前記復号鍵を初期値として前記第２のメモリにロードする第１のセレクタと、
前記第２のメモリ内の前記復号鍵に基づいて拡張鍵を計算すると共に、当該拡張鍵を前記第１のセレクタに送る復号化用拡張計算部を備え、
前記第１のセレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記復号化命令が、前記復号化装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記拡張鍵を前記第２のメモリにロードする、復号化装置。
【請求項８】
前記比較結果信号に基づいて前記トリガ信号を生成するトリガ信号生成器を更に備えた、請求項７記載の復号化装置。
【請求項９】
前記復号命令を発行すると共に、前記復号鍵の初期値に対応する前記フラグを第１のメモリに設定するプロセッサを更に備えた、請求項７記載の復号化装置。
【請求項１０】
前記第１のメモリは、前記復号鍵の初期値を保持すると共に、前記復号鍵の初期値を前記第１のセレクタへ出力するメモリと、前記フラグを保持すると共に、前記フラグを前記比較回路へ出力するメモリを有する、請求項７記載の復号化装置。
【請求項１１】
前記命令を発行すると共に、前記復号鍵の初期値に対応するフラグの対を複数第３のメモリに設定するプロセッサと、
前記プロセッサが発行する鍵選択信号に基づいて鍵の初期値に対応するフラグの対を１つ前記第１のメモリに設定する第２のセレクタを更に備えた、請求項７記載の復号化装置。
【請求項１２】
前記第２のメモリ内の前記第Ｎの拡張鍵～前記第１の拡張鍵によりデータを復号化するＡＥＳ（Advanced Encryption Standard）方式のエンジンを更に備えた、請求項７記載の暗号化装置。
【請求項１３】
データを記憶装置に記録し、前記記憶装置からデータを再生する制御を行う制御部と、
１つの暗号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用し、前記記憶装置に記録するデータを暗号化し、前記記憶装置から再生されたデータを復号化する暗号化及び復号化装置を備え、
前記暗号化及び復号化装置は、
鍵の初期値と対応するフラグを保持する第１のメモリと、

命令と、前記第１のメモリに保持された前記フラグが示す鍵が共に暗号化に関するものである場合、前記命令は暗号化命令でありかつ前記フラグが示す前記鍵は暗号鍵であり、或いは、前記命令と前記鍵が復号化に関するものである場合、前記命令は復号化命令でありかつ前記フラグが示す前記鍵は復号鍵である、そのような前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記鍵を初期値として前記第２のメモリにロードする第１のセレクタと、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記第１のセレクタに送る暗号化用拡張計算部と、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記第１のセレクタに送る復号化用拡張計算部を有し、
前記第１のセレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記暗号化命令が、当該記憶装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記暗号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードし、一方、前記復号化命令が、当該記憶装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記復号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードする、記憶装置。
【請求項１４】
前記暗号化及び復号化装置は、前記比較結果信号に基づいて前記トリガ信号を生成するトリガ信号生成器を更に有する、請求項１３記載の記憶装置。
【請求項１５】
前記命令を発行すると共に、前記鍵の初期値に対応する前記フラグを第１のメモリに設定するプロセッサを更に備えた、請求項１３記載の記憶装置。
【請求項１６】
前記第１のメモリは、前記鍵の初期値を保持すると共に、前記鍵の初期値を前記第１のセレクタへ出力するメモリと、前記フラグを保持すると共に、前記フラグを前記比較回路へ出力するメモリを有する、請求項１３記載の記憶装置。
【請求項１７】
前記命令を発行すると共に、前記鍵の初期値に対応するフラグの対を複数第３のメモリに設定するプロセッサと、
前記プロセッサが発行する鍵選択信号に基づいて鍵の初期値に対応するフラグの対を１つ前記第１のメモリに設定する第２のセレクタを更に備えた、請求項１３記載の記憶装置。
【請求項１８】
前記第２のメモリ内の前記第１の拡張鍵～前記第Ｎの拡張鍵によりデータを暗号化すると共に、前記第２のメモリ内の前記第Ｎの拡張鍵～前記第１の拡張鍵によりデータを復号化するＡＥＳ（Advanced Encryption Standard）方式のエンジンを更に備えた、請求項１３記載の記憶装置。
【請求項１９】
前記第１のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第２のメモリに設定され、
前記暗号化用拡張計算部又は前記復号化用拡張計算部による鍵拡張に由来する前記第２のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第１のメモリに設定され、
前記第１のメモリに設定された鍵の初期値に対応するフラグは、前記比較結果が不一致であることを示す場合に、前記第１のメモリを更新するために、前記第１のメモリに設定される、請求項１５記載の記憶装置。
【請求項２０】

前記第１のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第２のメモリに設定され、
前記暗号化用拡張計算部又は前記復号化用拡張計算部による鍵拡張に由来する前記第２のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第１のメモリに設定され、
前記第１のメモリに設定された鍵の初期値に対応するフラグは、前記比較結果が不一致であることを示す場合に、前記第１のメモリを更新するために、前記第１のメモリに設定される、請求項１７記載の記憶装置。
【請求項２１】
１つの暗号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用する暗号化及び復号化装置であって、
鍵の初期値に対応するフラグを保持する第１のメモリと、
命令と、前記第１のメモリに保持された前記フラグが示す鍵が共に暗号化に関するものである場合、前記命令は暗号化命令でありかつ前記フラグが示す前記鍵は暗号鍵であり、或いは、前記命令と前記鍵が復号化に関するものである場合、前記命令は復号化命令でありかつ前記フラグが示す前記鍵は復号鍵である、そのような前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記鍵を初期値として前記第２のメモリにロードするセレクタと、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記セレクタに送る暗号化用拡張計算部と、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記セレクタに送る復号化用拡張計算部を備え、
前記セレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記暗号化命令が、当該暗号化及び復号化装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記暗号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードし、一方、前記復号化命令が、当該暗号化及び復号化装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記復号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードする、暗号化及び復号化装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】変更
【補正の内容】
【００２６】
本発明の一観点によれば、１つの暗号鍵から拡張された、Ｎ（Ｎは２以上の自然数）個の拡張鍵を使用する暗号化装置であって、鍵の初期値に対応するフラグを保持する第１のメモリと、前記命令が暗号化命令でありかつ前記第１のメモリ内の前記フラグが示す鍵が前記暗号鍵である場合、前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、第２のメモリと、前記暗号化命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記暗号鍵を初期値として前記第２のメモリにロードする第１のセレクタと、前記第２のメモリ内の前記暗号鍵に基づいて前記拡張鍵を計算し、当該拡張鍵を前記第１のセレクタに送る暗号化用拡張計算部を備え、前記第１のセレクタは、初回に前記第２のメモリへ前記暗号鍵の初期値をロードし、前記暗号化命令が、前記暗号化装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記拡張鍵を前記第２のメモリにロードする、暗号化装置が提供される。
【手続補正３】

【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正の内容】
【００２７】
本発明の一観点によれば、１つの復号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用する復号化装置であって、鍵の初期値に対応するフラグを保持する第１のメモリと、前記命令が復号化命令であり、かつ、前記第１のメモリ内の前記フラグが示す鍵が前記復号鍵である場合、前記フラグ及び前記命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、第２のメモリと、前記復号化命令、トリガ信号及び前記比較結果信号に基づいて前記第１のメモリ内の前記復号鍵を初期値として前記第２のメモリにロードする第１のセレクタと、前記第２のメモリ内の前記復号鍵に基づいて拡張鍵を計算すると共に、当該拡張鍵を前記第１のセレクタに送る復号化用拡張計算部を備え、前記第１のセレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記復号化命令が、前記復号化装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記拡張鍵を前記第２のメモリにロードする、復号化装置が提供される。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】
本発明の一観点によれば、データを記憶装置に記録し、前記記憶装置からデータを再生する制御を行う制御部と、１つの暗号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用し、前記記憶装置に記録するデータを暗号化し、前記記憶装置から再生されたデータを復号化する暗号化及び復号化装置を備え、前記暗号化及び復号化装置は、鍵の初期値と対応するフラグを保持する第１のメモリと、命令と、前記第１のメモリに保持された前記フラグが示す鍵が共に暗号化に関するものである場合、前記命令は暗号化命令でありかつ前記フラグが示す前記鍵は暗号鍵であり、或いは、前記命令と前記鍵が復号化に関するものである場合、前記命令は復号化命令でありかつ前記フラグが示す前記鍵は復号鍵である、そのような前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、第２のメモリと、前記命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記鍵を初期値として前記第２のメモリにロードする第１のセレクタと、前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記第１のセレクタに送る暗号化用拡張計算部と、前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記第１のセレクタに送る復号化用拡張計算部を有し、前記第１のセレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記暗号化命令が、当該記憶装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記暗号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードし、一方、前記復号化命令が、当該記憶装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記復号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードする、記憶装置が提供される。
また、本発明の一観点によれば、１つの暗号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用する暗号化及び復号化装置であって、鍵の初期値に対応するフラグを保持する第１のメモリと、命令と、前記第１のメモリに保持された前記フラグが示す鍵が共に暗号化に関するものである場合、前記命令は暗号化命令でありかつ前記フラグが示す前記鍵は暗号鍵であり、或いは、前記命令と前記鍵が復号化に関するものである場合、前記命令は復号化命令でありかつ前記フラグが示す前記鍵は復号鍵である、そのような前記フラ

グ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、第２のメモリと、前記命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記鍵を初期値として前記第２のメモリにロードするセレクタと、前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記セレクタに送る暗号化用拡張計算部と、前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記セレクタに送る復号化用拡張計算部を備え、前記セレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記暗号化命令が、当該暗号化及び復号化装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記暗号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードし、一方、前記復号化命令が、当該暗号化及び復号化装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記復号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードする、暗号化及び復号化装置が提供される。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００７６
【補正方法】変更
【補正の内容】
【００７６】

以上の実施例を含む実施形態に関し、更に以下の付記を開示する。

（付記１）

１つの暗号鍵から拡張された、Ｎ（Ｎは２以上の自然数）個の拡張鍵を使用する暗号化装置であって、

鍵の初期値に対応するフラグを保持する第１のメモリと、

前記命令が暗号化命令でありかつ前記第１のメモリ内の前記フラグが示す鍵が前記暗号鍵である場合、前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、

第２のメモリと、

前記暗号化命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記暗号鍵を初期値として前記第２のメモリにロードする第１のセレクタと、

前記第２のメモリ内の前記暗号鍵に基づいて前記拡張鍵を計算し、当該拡張鍵を前記第１のセレクタに送る暗号化用拡張計算部を備え、

前記第１のセレクタは、初回に前記第２のメモリへ前記暗号鍵の初期値をロードし、前記暗号化命令が、前記暗号化装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記拡張鍵を前記第２のメモリにロードする、暗号化装置。

（付記２）

前記比較結果信号に基づいて前記トリガ信号を生成するトリガ信号生成器を更に備えた、付記１記載の暗号化装置。

（付記３）

前記暗号化命令を発行すると共に、前記暗号鍵の初期値に対応する前記フラグを第１のメモリに設定するプロセッサを更に備えた、付記１記載の暗号化装置。

（付記４）

前記第１のメモリは、前記暗号鍵の初期値を保持すると共に、前記暗号鍵の初期値を前記第１のセレクタへ出力するメモリと、前記フラグを保持すると共に、前記フラグを前記比較回路へ出力するメモリとを有する、付記１記載の暗号化装置。

（付記５）

前記命令を発行すると共に、前記暗号鍵の初期値に対応するフラグの対を複数第３のメモリに設定するプロセッサと、

前記プロセッサが発行する鍵選択信号に基づいて前記暗号鍵の初期値に対応するフラグ

の対を１つ前記第１のメモリに設定する第２のセレクタを更に備えた、付記１記載の暗号化装置。
（付記６）
前記第２のメモリ内の前記第１の拡張鍵～前記第Ｎの拡張鍵によりデータを暗号化するＡＥＳ（Advanced Encryption Standard）方式のエンジンを更に備えた、付記１記載の暗号化装置。
（付記７）
１つの復号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用する復号化装置であって、
鍵の初期値に対応するフラグを保持する第１のメモリと、
前記命令が復号化命令であり、かつ、前記第１のメモリ内の前記フラグが示す鍵が前記復号鍵である場合、前記フラグ及び前記命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記復号化命令、トリガ信号及び前記比較結果信号に基づいて前記第１のメモリ内の前記復号鍵を初期値として前記第２のメモリにロードする第１のセレクタと、
前記第２のメモリ内の前記復号鍵に基づいて拡張鍵を計算すると共に、当該拡張鍵を前記第１のセレクタに送る復号化用拡張計算部を備え、
前記第１のセレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記復号化命令が、前記復号化装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記拡張鍵を前記第２のメモリにロードする、復号化装置。
（付記８）
前記比較結果信号に基づいて前記トリガ信号を生成するトリガ信号生成器を更に備えた、付記７記載の復号化装置。
（付記９）
前記復号命令を発行すると共に、前記復号鍵の初期値に対応する前記フラグを第１のメモリに設定するプロセッサを更に備えた、付記７記載の復号化装置。
（付記１０）
前記第１のメモリは、前記復号鍵の初期値を保持すると共に、前記復号鍵の初期値を前記第１のセレクタへ出力するメモリと、前記フラグを保持すると共に、前記フラグを前記比較回路へ出力するメモリを有する、付記７記載の復号化装置。
（付記１１）
前記命令を発行すると共に、前記復号鍵の初期値に対応するフラグの対を複数第３のメモリに設定するプロセッサと、
前記プロセッサが発行する鍵選択信号に基づいて鍵の初期値に対応するフラグの対を１つ前記第１のメモリに設定する第２のセレクタを更に備えた、付記７記載の復号化装置。
（付記１２）
前記第２のメモリ内の前記第Ｎの拡張鍵～前記第１の拡張鍵によりデータを復号化するＡＥＳ（Advanced Encryption Standard）方式のエンジンを更に備えた、付記７記載の暗号化装置。
（付記１３）
データを記憶装置に記録し、前記記憶装置からデータを再生する制御を行う制御部と、
１つの暗号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用し、前記記憶装置に記録するデータを暗号化し、前記記憶装置から再生されたデータを復号化する暗号化及び復号化装置を備え、
前記暗号化及び復号化装置は、
鍵の初期値と対応するフラグを保持する第１のメモリと、
命令と、前記第１のメモリに保持された前記フラグが示す鍵が共に暗号化に関するものである場合、前記命令は暗号化命令でありかつ前記フラグが示す前記鍵は暗号鍵であり、

或いは、前記命令と前記鍵が復号化に関するものである場合、前記命令は復号化命令でありかつ前記フラグが示す前記鍵は復号鍵である、そのような前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記鍵を初期値として前記第２のメモリにロードする第１のセレクタと、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記第１のセレクタに送る暗号化用拡張計算部と、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記第１のセレクタに送る復号化用拡張計算部を有し、
前記第１のセレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記暗号化命令が、当該記憶装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記暗号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードし、一方、前記復号化命令が、当該記憶装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記復号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードする、記憶装置。
（付記１４）
前記暗号化及び復号化装置は、前記比較結果信号に基づいて前記トリガ信号を生成するトリガ信号生成器を更に有する、付記１３記載の記憶装置。
（付記１５）
前記命令を発行すると共に、前記鍵の初期値に対応する前記フラグを第１のメモリに設定するプロセッサを更に備えた、付記１３記載の記憶装置。
（付記１６）
前記第１のメモリは、前記鍵の初期値を保持すると共に、前記鍵の初期値を前記第１のセレクタへ出力するメモリと、前記フラグを保持すると共に、前記フラグを前記比較回路へ出力するメモリを有する、付記１３記載の記憶装置。
（付記１７）
前記命令を発行すると共に、前記鍵の初期値に対応するフラグの対を複数第３のメモリに設定するプロセッサと、
前記プロセッサが発行する鍵選択信号に基づいて鍵の初期値に対応するフラグの対を１つ前記第１のメモリに設定する第２のセレクタを更に備えた、付記１３記載の記憶装置。
（付記１８）
前記第２のメモリ内の前記第１の拡張鍵～前記第Ｎの拡張鍵によりデータを暗号化すると共に、前記第２のメモリ内の前記第Ｎの拡張鍵～前記第１の拡張鍵によりデータを復号化するＡＥＳ（Advanced Encryption Standard）方式のエンジンを更に備えた、付記１３記載の記憶装置。
（付記１９）
前記第１のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第２のメモリに設定され、
前記暗号化用拡張計算部又は前記復号化用拡張計算部による鍵拡張に由来する前記第２のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第１のメモリに設定され、
前記第１のメモリに設定された鍵の初期値に対応するフラグは、前記比較結果が不一致であることを示す場合に、前記第１のメモリを更新するために、前記第１のメモリに設定される、付記１５記載の記憶装置。
（付記２０）
前記第１のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第２のメモリに設定され、
前記暗号化用拡張計算部又は前記復号化用拡張計算部による鍵拡張に由来する前記第２

のメモリ内の鍵の初期値は、前記比較結果が不一致であることを示す場合に、前記第１のメモリに設定され、
前記第１のメモリに設定された鍵の初期値に対応するフラグは、前記比較結果が不一致であることを示す場合に、前記第１のメモリを更新するために、前記第１のメモリに設定される、付記１７記載の記憶装置。
（付記２１）
１つの暗号鍵に由来するＮ（Ｎは２以上の自然数）個の拡張鍵を使用する暗号化及び復号化装置であって、
鍵の初期値に対応するフラグを保持する第１のメモリと、
命令と、前記第１のメモリに保持された前記フラグが示す鍵が共に暗号化に関するものである場合、前記命令は暗号化命令でありかつ前記フラグが示す前記鍵は暗号鍵であり、或いは、前記命令と前記鍵が復号化に関するものである場合、前記命令は復号化命令でありかつ前記フラグが示す前記鍵は復号鍵である、そのような前記フラグ及び命令が対応するものであるかどうかを示す比較結果信号を出力する比較回路と、
第２のメモリと、
前記命令、トリガ信号及び前記比較結果信号に基づいて、前記第１のメモリ内の前記鍵を初期値として前記第２のメモリにロードするセレクタと、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記セレクタに送る暗号化用拡張計算部と、
前記第２のメモリ内の鍵に基づいて前記拡張鍵を計算すると共に、前記拡張鍵を前記セレクタに送る復号化用拡張計算部を備え、
前記セレクタは、初回に前記第２のメモリへ前記鍵の初期値をロードし、前記暗号化命令が、当該暗号化及び復号化装置に指示して、第１の拡張鍵～第Ｎの拡張鍵の順に、前記暗号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記暗号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードし、一方、前記復号化命令が、当該暗号化及び復号化装置に指示して、第Ｎの拡張鍵～第１の拡張鍵の順に、前記復号鍵を前記拡張鍵に拡張させる場合は、前記初回の後前記復号化用拡張計算部で計算された拡張鍵を前記第２のメモリにロードする、暗号化及び復号化装置。