【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26年4月17日(2014.4.17)

【公開番号】特開2014-41382(P2014-41382A)
【公開日】平成26年3月6日(2014.3.6)
【年通号数】公開・登録公報2014-012
【出願番号】特願2013-222466(P2013-222466)
【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26年2月10日(2014.2.10)
【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】
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）アルゴリズムのＡＥＳラウンドを実行するための第１の命令であって、前記ＡＥＳラウンドのための入力データを含むソースオペランドと、前記ＡＥＳラウンドのためのラウンド鍵を含むソースオペランドとを有する第１の命令を受信する復号化部と、
前記復号化部に連結された実行部であって、前記第１の命令に応じて、前記ＡＥＳラウンドによって前記ラウンド鍵を用いて変換された前記入力データを含む結果を、前記第１の命令のｄｅｓｔｉｎａｔｉｏｎに格納する実行部と
を備えるプロセッサ。
【請求項２】
前記第１の命令は、ＡＥＳ暗号化ラウンドを実行するための命令である、請求項１に記載のプロセッサ。
【請求項３】
前記第１の命令は、ＡＥＳ復号化ラウンドを実行するための命令である、請求項１に記載のプロセッサ。
【請求項４】
前記入力データを含むための前記ソースオペランドは、レジスタに格納され、
前記ラウンド鍵を含むための前記ソースオペランドは、レジスタに格納される、請求項１に記載のプロセッサ。
【請求項５】
前記レジスタは、１２８ビットレジスタである、請求項４に記載のプロセッサ。
【請求項６】
前記実行部は、前記第１の命令に応じて、前記入力データを前記結果で上書きする、請求項１から５のいずれか一項に記載のプロセッサ。
【請求項７】
前記実行部は、前記第１の命令に応じて、Ｓ－ボックスルックアップ、行シフト、列混合、及びラウンド鍵加算を実行する、請求項１に記載のプロセッサ。
【請求項８】
前記復号化部は、前記ＡＥＳラウンドのための前記ラウンド鍵を生成するための第２の

命令であって、前のＡＥＳラウンドのための前のラウンド鍵を含むソースオペランドを有する第２の命令を受信し、
前記プロセッサは、
前記第２の命令に応じて、前記前のラウンド鍵に基づいて前記ＡＥＳラウンドのための前記ラウンド鍵を生成する鍵スケジューラ
をさらに備える、請求項１に記載のプロセッサ。
【請求項９】
前記第２の命令は、即値を有し、
前記鍵スケジューラは、前記前のラウンド鍵及び前記即値に基づいて前記ＡＥＳラウンドのための前記ラウンド鍵を生成し、
前記第２の命令は、前記第１の命令とは異なるｏｐｃｏｄｅを有する、
請求項８に記載のプロセッサ。
【請求項１０】
前記復号化部は、前記ＡＥＳアルゴリズムの最終ＡＥＳラウンドを実行するための第３の命令であって、前記最終ＡＥＳラウンドのための入力データを含むソースオペランドと、前記最終ＡＥＳラウンドのための最終ラウンド鍵を含むソースオペランドとを有する第３の命令を受信し、
前記実行部は、前記第３の命令に応じて、前記最終ＡＥＳラウンドによって前記最終ＡＥＳラウンドのための前記最終ラウンド鍵を用いて変換された前記最終ＡＥＳラウンドのための前記入力データを含む第２の結果を、前記第３の命令のｄｅｓｔｉｎａｔｉｏｎに格納し、
前記第２の命令は前記第１の命令とは異なるｏｐｃｏｄｅを有する、請求項１に記載のプロセッサ。
【請求項１１】
前記プロセッサは、汎用プロセッサである、請求項１から１０のいずれか一項に記載のプロセッサ。
【請求項１２】
複数の１２８ビットレジスタと、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号化ラウンドを実行するための命令であって、前記複数の１２８ビットレジスタのうちの暗号化される情報を含む第１の１２８ビットレジスタを示し、前記複数の１２８ビットレジスタのうちの前記ＡＥＳ暗号化ラウンドのためのラウンド鍵を含む第２の１２８ビットレジスタを示す命令を受信する復号化部と、
前記復号化部及び前記複数の１２８ビットレジスタに連結された実行部であって、前記命令に応じて、前記ラウンド鍵を用いて前記ＡＥＳ暗号化ラウンドによって変換された前記第１の１２８ビットレジスタからの前記情報を含む結果を、前記命令のｄｅｓｔｉｎａｔｉｏｎに格納する実行部と
を備えるプロセッサ。
【請求項１３】
前記実行部は、前記命令に応じて、Ｓ－ボックスルックアップ、行シフト、列混合、及びラウンド鍵加算を実行する、請求項１２に記載のプロセッサ。
【請求項１４】
前記プロセッサは、汎用プロセッサである、請求項１２又は１３に記載のプロセッサ。
【請求項１５】
複数の１２８ビットレジスタと、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）復号化ラウンドを実行する命令であって、前記複数の１２８ビットレジスタのうちの復号化される情報を含む第１の１２８ビットレジスタを示し、前記複数の１２８ビットレジスタのうちの前記ＡＥＳ復号化ラウンドのためのラウンド鍵を含む第２の１２８ビットレジスタを示す命令を受信する復号化部と、

前記復号化部及び前記複数の１２８ビットレジスタに連結された実行部であって、前記命令に応じて、前記ＡＥＳ復号化ラウンドによって前記ラウンド鍵を用いて変換された前記第１の１２８ビットレジスタからの前記情報を含む結果を、前記命令のｄｅｓｔｉｎａｔｉｏｎに格納する実行部と
を備えるプロセッサ。
【請求項１６】
前記プロセッサは、汎用プロセッサである、請求項１５に記載のプロセッサ。
【請求項１７】
ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）ラウンドのためのラウンド鍵を生成するための命令であって、前のＡＥＳラウンドのための前のラウンド鍵を含むソースオペランドを有する命令を受信する復号化部と、
前記復号化部に連結された鍵スケジューラであって、前記命令に応じて、前記ＡＥＳラウンドのための前記ラウンド鍵を前記命令のｄｅｓｔｉｎａｔｉｏｎに格納する鍵スケジューラと
を備えるプロセッサ。
【請求項１８】
前記命令は即値を有し、
前記鍵スケジューラは、前記即値に基づいて前記ＡＥＳラウンドのための前記ラウンド鍵を生成し、
前記ｄｅｓｔｉｎａｔｉｏｎは、１２８ビットレジスタである、
請求項１７に記載のプロセッサ。
【請求項１９】
第１のＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）暗号化ラウンドのための第１ラウンド鍵を生成するための第１の命令であって、前記第１ラウンド鍵の生成に用いる鍵を含む第１命令ソースオペランドを有する第１の命令と、
第２のＡＥＳ暗号化ラウンドを実行するための第２の命令であって、前記第２のＡＥＳ暗号化ラウンドのための入力データを含む第２命令第１ソースオペランドを有し、前記第２のＡＥＳ暗号化ラウンドのための第２ラウンド鍵を含む第２命令第２ソースオペランドを有する第２の命令と、
ＡＥＳ暗号化最終ラウンドを実行するための第３の命令であって、前記ＡＥＳ暗号化最終ラウンドのための入力データを含む第３命令第１ソースオペランドを有し、前記ＡＥＳ暗号化最終ラウンドのための最終ラウンド鍵を含む第３命令第２ソースオペランドを有する第３の命令と
を少なくとも含む複数の命令を受信して復号化する復号化部と、
前記第１の命令に応じて、前記第１命令ソースオペランドからの前記鍵に基づいて、前記第１のＡＥＳ暗号化ラウンドのための前記第１ラウンド鍵を生成する鍵スケジューラと、
前記復号化部に連結され、前記第２の命令に応じて、前記第２のＡＥＳ暗号化ラウンドによって前記第２ラウンド鍵を用いて変換された前記第２のＡＥＳ暗号化ラウンドのための前記入力データを含む前記第２の命令の結果を、前記第２の命令のｄｅｓｔｉｎａｔｉｏｎに格納し、前記第３の命令に応じて、前記ＡＥＳ暗号化最終ラウンドによって前記最終ラウンド鍵を用いて変換された前記ＡＥＳ暗号化最終ラウンドのための前記入力データを含む前記第３の命令の結果を、前記第３の命令のｄｅｓｔｉｎａｔｉｏｎに格納する実行部と
を備えるプロセッサ。
【請求項２０】
前記第１の命令は、第１ｏｐｃｏｄｅを有し、前記第２の命令は、前記第１ｏｐｃｏｄｅとは異なる第２ｏｐｃｏｄｅを有し、前記第３の命令は、前記第１ｏｐｃｏｄｅ及び前記第２ｏｐｃｏｄｅとは異なる第３ｏｐｃｏｄｅを有する、請求項１９に記載のプロセッサ。

【請求項２１】
前記第１の命令は即値を有し、
前記鍵スケジューラは、前記即値に基づいて、前記第１ラウンド鍵を生成する、請求項１９に記載のプロセッサ。
【請求項２２】
前記プロセッサは、汎用プロセッサである、請求項１９から２１のいずれか一項に記載のプロセッサ。
【請求項２３】
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド暗号化演算を実行するべく、１２８ビットの入力データを格納する宛先レジスタ及び１２８ビットのラウンド鍵を格納するソースレジスタを特定するシングルラウンド暗号化命令を復号化する復号化部と、
前記シングルラウンド暗号化命令に基づいてマイクロ演算を実行する実行部であって、前記１２８ビットの入力データ及び前記１２８ビットのラウンド鍵を受信し、前記ラウンド鍵を用いて前記１２８ビットの入力データに対して前記ＡＥＳシングルラウンド暗号化演算を実行し、１２８ビットの結果データを前記宛先レジスタに格納する実行部と
を備えるプロセッサ。
【請求項２４】
プロセッサであって、
１２８ビットの入力データを格納する第１の１２８ビットレジスタ及び１２８ビットのラウンド鍵を格納する第２の１２８ビットレジスタを含むレジスタファイルと、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド暗号化演算を実行するべく、前記第１の１２８ビットレジスタ及び前記第２の１２８ビットレジスタを特定するシングルラウンド暗号化命令を復号化する復号化部と、
複数のポートであって、それぞれに、整数演算又は浮動小数点演算をパラレルにサポートするための１以上の実行リソースが関連付けられた複数のポートと、
前記複数のポートのうちの選択されたポートに、前記ＡＥＳシングルラウンド暗号化演算を発行する発行制御ロジックと
を備え、
前記選択されたポートに関連付けられた前記１以上の実行リソースは、前記１２８ビットのラウンド鍵を用いて前記１２８ビットの入力データに対して前記シングルラウンド暗号化演算を実行し、前記第１の１２８ビットレジスタに格納する１２８ビット出力データを生成するためのものである、プロセッサ。
【請求項２５】
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド復号化演算を実行するべく、１２８ビットの入力データを格納する宛先レジスタ及び１２８ビットのラウンド鍵を格納するソースレジスタを特定するシングルラウンド復号化命令を復号化する復号化部と、
前記シングルラウンド復号化命令に基づいてマイクロ演算を実行する実行部であって、前記１２８ビットの入力データ及び前記１２８ビットのラウンド鍵を受信し、前記ラウンド鍵を用いて前記１２８ビットの入力データに対してＡＥＳシングルラウンド復号化演算を実行し、１２８ビットの結果データを前記宛先レジスタに格納する実行部と
を備えるプロセッサ。
【請求項２６】
プロセッサであって、
１２８ビットの入力データを格納する第１の１２８ビットレジスタ及び１２８ビットのラウンド鍵を格納する第２の１２８ビットレジスタを含むレジスタファイルと、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド復号化演算を実行するべく、前記第１の１２８ビットレジスタ及び前記第２の１２８ビットレジスタを特定するシングルラウンド復号化命令を復号化する復号化部と、

複数のポートであって、それぞれに、整数演算又は浮動小数点演算をパラレルにサポートするための１以上の実行リソースが関連付けられた複数のポートと、
前記複数のポートのうちの選択されたポートに、前記ＡＥＳシングルラウンド復号化演算を発行する発行制御ロジックと
を備え、
前記選択されたポートに関連付けられた前記１以上の実行リソースは、前記１２８ビットのラウンド鍵を用いて前記１２８ビットの入力データに対して前記シングルラウンド復号化演算を実行し、前記第１の１２８ビットレジスタに格納する１２８ビット出力データを生成するためのものである、プロセッサ。
【請求項２７】
格納デバイスと、
前記格納デバイスとの通信を制御する格納Ｉ／Ｏコントローラと、
ダブルデータレートＲＡＭと、
前記ダブルデータレートＲＡＭとの通信を制御するメモリコントローラと、
前記格納Ｉ／Ｏコントローラ及び前記メモリコントローラに接続されたプロセッサであって、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド暗号化演算を実行するべく、１２８ビットの入力データを格納する宛先レジスタ及び１２８ビットのラウンド鍵を格納するソースレジスタを特定するシングルラウンド暗号化命令を復号化する復号化部と、
前記シングルラウンド暗号化命令に基づいてマイクロ演算を実行する実行部であって、前記１２８ビットの入力データ及び前記１２８ビットのラウンド鍵を受信し、前記ラウンド鍵を用いて前記１２８ビットの入力データに対してＡＥＳシングルラウンド暗号化演算を実行し、１２８ビットの結果データを前記宛先レジスタに格納する実行部と
を有するプロセッサと
を備えるシステム。
【請求項２８】
格納デバイスと、
前記格納デバイスとの通信を制御する格納Ｉ／Ｏコントローラと、
ダブルデータレートＲＡＭと、
前記ダブルデータレートＲＡＭとの通信を制御するメモリコントローラと、
前記格納Ｉ／Ｏコントローラ及び前記メモリコントローラに接続されたプロセッサであって、
１２８ビットの入力データを格納する第１の１２８ビットレジスタ及び１２８ビットのラウンド鍵を格納する第２の１２８ビットレジスタを含むレジスタファイルと、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド暗号化演算を実行するべく、前記第１の１２８ビットレジスタ及び前記第２の１２８ビットレジスタを特定するシングルラウンド暗号化命令を復号化する復号化部と、
複数のポートであって、それぞれに、整数演算又は浮動小数点演算をパラレルにサポートするための１以上の実行リソースが関連付けられた複数のポートと、
前記複数のポートのうちの選択されたポートに、前記ＡＥＳシングルラウンド暗号化演算を発行する発行制御ロジックと
を有し、
前記選択されたポートに関連付けられた前記１以上の実行リソースは、前記１２８ビットのラウンド鍵を用いて前記１２８ビットの入力データに対して前記シングルラウンド暗号化演算を実行し、前記第１の１２８ビットレジスタに格納する１２８ビット出力データを生成するためのものである、プロセッサと
を備えるシステム。
【請求項２９】
格納デバイスと、

前記格納デバイスとの通信を制御する格納Ｉ／Ｏコントローラと、
ダブルデータレートＲＡＭと、
前記ダブルデータレートＲＡＭとの通信を制御するメモリコントローラと、
前記格納Ｉ／Ｏコントローラ及び前記メモリコントローラに接続されたプロセッサであって、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド復号化演算を実行するべく、１２８ビットの入力データを格納する宛先レジスタ及び１２８ビットのラウンド鍵を格納するソースレジスタを特定するシングルラウンド復号化命令を復号化する復号化部と、
前記シングルラウンド復号化命令に基づいてマイクロ演算を実行する実行部であって、前記１２８ビットの入力データ及び前記１２８ビットのラウンド鍵を受信し、前記ラウンド鍵を用いて前記１２８ビットの入力データに対してＡＥＳシングルラウンド復号化演算を実行し、１２８ビットの結果データを前記宛先レジスタに格納する実行部と
を有するプロセッサと
を備えるシステム。
【請求項３０】
格納デバイスと、
前記格納デバイスとの通信を制御する格納Ｉ／Ｏコントローラと、
ダブルデータレートＲＡＭと、
前記ダブルデータレートＲＡＭとの通信を制御するメモリコントローラと、
前記格納Ｉ／Ｏコントローラ及び前記メモリコントローラに接続されたプロセッサであって、
１２８ビットの入力データを格納する第１の１２８ビットレジスタ及び１２８ビットのラウンド鍵を格納する第２の１２８ビットレジスタを含むレジスタファイルと、
ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）シングルラウンド復号化演算を実行するべく、前記第１の１２８ビットレジスタ及び前記第２の１２８ビットレジスタを特定するシングルラウンド復号化命令を復号化する復号化部と、
複数のポートであって、それぞれに、整数演算又は浮動小数点演算をパラレルにサポートするための１以上の実行リソースが関連付けられた複数のポートと、
前記複数のポートのうちの選択されたポートに、前記ＡＥＳシングルラウンド復号化演算を発行する発行制御ロジックと
を有し、
前記選択されたポートに関連付けられた前記１以上の実行リソースは、前記１２８ビットのラウンド鍵を用いて前記１２８ビットの入力データに対して前記シングルラウンド復号化演算を実行し、前記第１の１２８ビットレジスタに格納する１２８ビット出力データを生成するためのものである、プロセッサと
を備えるシステム。