(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-520517
(P2010-520517A)
(43)公表日　平成22年6月10日(2010.6.10)

(51)Int.Cl.	F I		テーマコード（参考）
G09C 1/00 (2006.01)	G09C	1/00 610A	5J104

審査請求 有　予備審査請求 未請求　（全 25 頁）

(21)出願番号　特願2009-552935 (P2009-552935)
(86)(22)出願日　平成20年3月25日 (2008.3.25)
(85)翻訳文提出日　平成21年9月3日 (2009.9.3)
(86)国際出願番号　PCT/US2008/058128
(87)国際公開番号　WO2008/121614
(87)国際公開日　平成20年10月9日 (2008.10.9)
(31)優先権主張番号　11/729,199
(32)優先日　平成19年3月28日 (2007.3.28)
(33)優先権主張国　米国 (US)

(71)出願人　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　ゲロン、シェイ
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

最終頁に続く

(54)【発明の名称】新暗号規格（ＡＥＳ）向けの柔軟なアーキテクチャおよび命令

(57)【要約】
汎用プロセッサ用の柔軟なＡＥＳ命令セットが提供される。命令セットは、ＡＥＳ暗号化または復号化用に「１ラウンド」パスを行う命令を含み、さらに、鍵生成を行う命令を含む。１２８／１９２／２５６ビット鍵用の鍵生成の鍵サイズおよびラウンド数を示すのに直近を利用してよい。柔軟なＡＥＳ命令セットは、暗黙のレジスタをトラッキングする必要がないので、パイプライン能力の最大限の発揮が可能である。
【選択図】図１

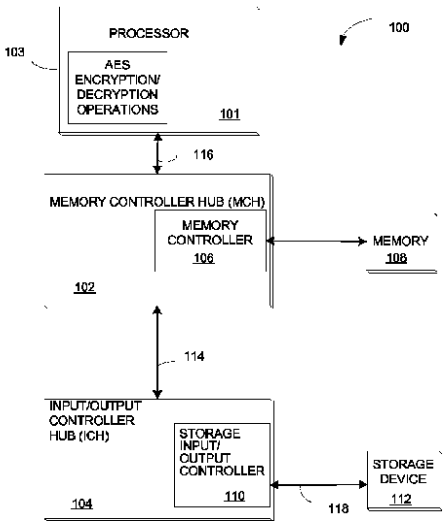


FIG. 1

【特許請求の範囲】
【請求項１】
ＡＥＳ命令の一連の演算を行う実行部を備える装置であって、
前記一連の演算は、プラグラム可能な数のＡＥＳラウンドを行い、
前記演算は前記実行部に、
前記ＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードさせ、
各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成させ、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行わせて、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供させる、装置。
【請求項２】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記実行部は、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする、請求項１に記載の装置。
【請求項３】
前記一連のＡＥＳラウンド演算により、前記実行部は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成し、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行い、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う、請求項２に記載の装置。
【請求項４】
前記ＡＥＳラウンドの数－１に対して前記一連のＡＥＳラウンド演算を行うことで、前記実行部は、
前記ＡＥＳラウンドの前記入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成し、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行い、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行い、
前記置換演算の結果に、前記中間値の列同士を混合させるビット線形変換を行う、請求項１に記載の装置。
【請求項５】
最終ラウンドに前記一連のＡＥＳラウンド演算を行うことで、前記実行部は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成し、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行い、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う、請求項４に記載の装置。
【請求項６】
前記結果は暗号化された値である、請求項１に記載の装置。
【請求項７】
前記結果は復号化された値である、請求項１に記載の装置。
【請求項８】
第１のＡＥＳラウンドの鍵および入力がレジスタファイルに格納されている、請求項１に記載の装置。
【請求項９】
前記レジスタファイルは複数の１２８ビットレジスタを含む、請求項８に記載の装置。

【請求項１０】
ＡＥＳ命令のプログラム可能なＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードして、各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成する段階と、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行い、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供する段階と、を備える方法。
【請求項１１】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする段階を備える、請求項１０に記載の方法。
【請求項１２】
前記一連のＡＥＳラウンド演算を行う段階は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成する段階と、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行う段階と、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う段階と、を有する、請求項１１に記載の方法。
【請求項１３】
前記ラウンドの数１に対して前記一連のＡＥＳラウンド演算を行う段階は、
前記ＡＥＳラウンドの前記入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成する段階と、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行う段階と、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う段階と、
前記置換演算の結果に、前記中間値の列同士を混合させるビット線形変換を行う段階と、を有する、請求項１０に記載の方法。
【請求項１４】
最終ＡＥＳラウンドに前記一連のＡＥＳラウンド演算を行う段階は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成する段階と、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行う段階と、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う段階と、を有する、請求項１３に記載の方法。
【請求項１５】
前記結果は暗号化された値である、請求項１０に記載の方法。
【請求項１６】
前記結果は復号化された値である、請求項１０に記載の方法。
【請求項１７】
第１のＡＥＳラウンドの鍵および入力がレジスタファイルに格納されている、請求項１０に記載の方法。
【請求項１８】
前記レジスタファイルは複数の１２８ビットレジスタを含む、請求項１７に記載の方法。
【請求項１９】
関連情報を有する機械アクセス可能な媒体を含む物品であって、前記情報はアクセスされると機械に、
ＡＥＳ命令のプログラム可能なＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵

レジスタにロードさせ、各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成させ、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行わせて、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供させる、物品。
【請求項２０】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵がロードされる、請求項１９に記載の物品。
【請求項２１】
データおよび命令を格納するダイナミックランダムアクセスメモリと、
前記メモリに連結されて前記命令を実行するプロセッサと、を備えるシステムであって、
前記プロセッサは、
ＡＥＳ命令の一連の演算を行う実行部を備え、
前記一連の演算は、プラグラム可能な数のＡＥＳラウンドを行い、
前記演算は前記実行部に、
前記ＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードさせ、
各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成させ、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行わせて、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供させる、システム。
【請求項２２】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記実行部は、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする、請求項２１に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、暗号化アルゴリズムに係り、特に、新暗号規格（ＡＥＳ）アルゴリズムに係る。
【背景技術】
【０００２】
暗号学はアルゴリズムに依存するツールであり、情報保護における要諦である。アルゴリズムは、複雑な数学的アルゴリズムであり、ビット列がその要諦である。暗号システムには、秘密鍵システムと公開鍵システムという２つの基本的な種類がある。秘密鍵システムは、２以上の当事者間で共有される単一の鍵（「秘密鍵」）を有する対称システムとも称される。単一の鍵は、情報の暗号化および復号化両方に用いられる。
【０００３】
(米国)標準技術局（ＮＩＳＴ）がＦＩＰＳ（Federal Information Processing Standard）１９７として刊行した新暗号規格（ＡＥＳ）は秘密鍵システムである。ＡＥＳは、情報の暗号化および復号化を行うことのできる対称ブロック暗号である。
【０００４】
暗号化は、秘密鍵（暗号鍵）を用いて一連の変換を行うことで、「平文」と称される理解可能なデータを「暗号文」と称される理解不能な形式に変換する。暗号の変換は、（１）排他的論理和（ＸＯＲ）演算を用いて、ラウンド鍵（暗号鍵から得られる値）を、状態（２次元のバイト列）に加算すること、（２）非線形バイト置換テーブル（Ｓ－Ｂｏｘ）を用いて状態を処理すること、（３）状態の最後の３行を異なるオフセットで周期的にシフトすること、および（４）状態の全ての列を取り出して、そのデータを（互いに独立し

て）混合して、新たな列を作成すること、を含む。
【０００５】
復号化（逆暗号化）は、暗号鍵を用いて一連の変化を行うことで、「暗号文」ブロックを、同じサイズの「平文」ブロックに変換する。逆暗号化における変換は、暗号化における変換の逆の処理である。
【０００６】
ＡＥＳ規格では、１２８ビットのデータブロックの処理に、長さが１２８、１９２、および２５６ビットの暗号鍵を用いるラインデールアルゴリズムを指定する。異なる鍵の長さは、通常、ＡＥＳ－１２８、ＡＥＳ－１９２、およびＡＥＳ－２５６と称される。
【０００７】
ＡＥＳアルゴリズムは、平文を暗号文に、または暗号文を平文に、１０、１２、または１４個の連続したラウンドで変換し、ラウンド数は鍵の長さに依存している。
【図面の簡単な説明】
【０００８】
請求されている主題の実施形態の特徴は、以下の詳細な記載を、図面を参照して読むことで明らかになるが、図面において同様の要素には同様の参照番号が付されている。
【図１】本発明の原理による、汎用プロセッサにおいてＡＥＳ暗号化および復号化を行う柔軟なアーキテクチャおよび命令の一実施形態を含むシステムのブロック図である。
【図２】図１に示すプロセッサの一実施形態のブロック図である。
【図３】本発明の原理による、ＡＥＳ暗号化および復号化を行う図２に示す実行部の一実施形態を含むブロック図である。
【図４】図３の実行部によるＡＥＳ暗号化ラウンド命令のフローを示すフローグラフである。
【図５】図３の実行部によるＡＥＳ暗号化最終ラウンド命令のフローを示すフローグラフである。
【図６】図３の実行部によるＡＥＳ復号化ラウンド命令のフローを示すフローグラフである。
【図７】図３の実行部によるＡＥＳ復号化最終ラウンド命令のフローを示すフローグラフである。
【図８】ラウンド鍵を生成し暗号化および復号化を行うのに利用されうる直近のバイトを有するＡＥＳラウンド命令の一実施形態を示す。　以下の詳細な記載は、請求されている主題の例示的な実施形態を参照しながら述べるが、当業者には多くの代替例、変形例、および変更例が明らかである。故に、請求されている主題は広義に解釈されることが意図されており、添付請求項で定義が行われることが意図されている。
【発明を実施するための形態】
【０００９】
新暗号規格（ＡＥＳ）アルゴリズムは、通常ソフトウェアまたは専用プロセッサで実行されるコンピューティング集約型のアルゴリズムである。故にこの暗号化は、通常、コンピュータに格納されている情報のサブセット（「トップシークレット」として機密扱いされうるような類の情報等）の暗号化に限って利用されている。しかし、コンピュータに格納されている情報を今まで以上に暗号化する必要がでてきている。例えば、携帯コンピュータに格納されている全ての情報が暗号化されれば、携帯コンピュータの盗難に際しても情報保護が可能となる。
【００１０】
ＡＥＳは、１２８、１９２、または２５６ビットのサイズの鍵を用いて、１２８ビットブロックに施されるブロック暗号である。鍵のサイズに応じて、演算列を多くのラウンド（１０、１２、または１４）について繰り返す。
【００１１】
各ラウンドにおける鍵の生成は、ラウンド鍵を格納する暗黙の１２８ビットレジスタを利用して、その都度（on the fly）（つまり各ラウンド直前に）行われてよい。しかし、

暗黙のレジスタの利用により、前の命令結果に対する依存性から、ｘ８６レジスタベースのプロセッサの性能が低下する虞がある。

【００１２】

例えば、アプリケーションによっては、フロー毎に異なる鍵を有しうるネットワークパケットを処理するためその都度鍵生成することが好都合なものもある。一方で、例えばディスクドライブのコンテンツを暗号化／復号化するのに用いられる単一の鍵に多くの性能が必要とされる類のアプリケーションもある。このように、鍵生成には柔軟性が求められる。本発明の一実施形態は、汎用プロセッサでＡＥＳ暗号化および復号化を行う柔軟なアーキテクチャおよび命令を提供する。

【００１３】

図１は、本発明の原理による、汎用プロセッサにおいてＡＥＳ暗号化および復号化を行う柔軟なアーキテクチャおよび命令の一実施形態を含むシステム１００のブロック図である。システム１００は、プロセッサ１０１、メモリコントローラハブ（ＭＣＨ）またはグラフィックメモリハブ（ＧＭＣＨ）１０２、および入出力（Ｉ／Ｏ）コントローラハブ（ＩＣＨ）１０４を含む。ＭＣＨ１０２は、プロセッサ１０１とメモリ１０８との間の通信を制御するメモリコントローラ１０６を含む。プロセッサ１０１とＭＣＨ１０２とは、システムバス１１６を介して通信する。

【００１４】

プロセッサ１０１は、シングルコアＩｎｔｅｌ（登録商標）Ｐｅｎｔｉｕｍ（登録商標）　ＩＶ（登録商標）プロセッサ、シングルコアＩｎｔｅｌ　Ｃｅｌｅｒｏｎプロセッサ、Ｉｎｔｅｌ（登録商標）ＸＳｃａｌｅプロセッサ、または、Ｉｎｔｅｌ（登録商標）Ｐｅｎｔｉｕｍ（登録商標）　Ｄ、Ｉｎｔｅｌ（登録商標）Ｘｅｏｎ（登録商標）プロセッサ等のマルチコアプロセッサ、または、Ｉｎｔｅｌ（登録商標）Ｃｏｒｅ（登録商標）Ｄｕｏプロセッサ、または任意の他の種類のプロセッサ等の複数のプロセッサのいずれかであってよい。

【００１５】

メモリ１０８は、ダイナミックＲＡＭ（ＤＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、シンクロナスＤＲＡＭ（ＳＤＲＡＭ）、ダブルデータレート２（ＤＤＲ２）ＲＡＭ、またはランバスＤＲＡＭ（ＲＤＲＡＭ）、または任意の他の種類のメモリであってよい。

【００１６】

ＩＣＨ１０４は、ディレクトメディアインタフェース（ＤＭＩ）等の高速チップツーチップインターコネクト１１４を用いてＭＣＨ１０２に連結されてよい。ＤＭＩは、２ギガビット／秒の同時転送レートを２つの単方向レーンによりサポートする。

【００１７】

ＩＣＨ１０４は、ＩＣＨ１０４に連結された少なくとも１つの格納デバイス１１２との通信を制御する格納Ｉ／Ｏコントローラ１１０を含みうる。格納デバイスは、例えば、ディスクドライブ、デジタルビデオディスク（ＤＶＤ）ドライブ、コンパクトディスク（ＣＤ）ドライブ、ＲＡＩＤ（Redundant Array of Independent Disks）、テープドライブまたは他の格納デバイスであってよい。ＩＣＨ１０４は、格納プロトコルインターコネクト１１８を介して、ＳＡＳ（Serial Attached Small Computer System Interface）またはＳＡＴＡ（Serial Advanced Technology Attachment)等のシリアル格納プロトコルを用いて格納デバイス１１２と通信しうる。

【００１８】

プロセッサ１０１は、ＡＥＳ暗号化および復号化演算を行うＡＥＳ機能１０３を含む。ＡＥＳ機能１０３は、メモリ１０８に格納されている、および／または、格納デバイス１１２に格納されている情報の暗号化または復号化に利用されうる。

【００１９】

図２は、図１に示すプロセッサ１０１の一実施形態のブロック図である。プロセッサ１０１は、レベル１（Ｌ１）命令キャッシュ２０２から受信したプロセッサ命令を復号化するフェッチ復号化部２０６を含む。命令実行に利用されるデータはレジスタファイル２０

８に格納されていてよい。一実施形態においては、レジスタファイル２０８は、複数の１２８ビットレジスタを含み、これらは、ＡＥＳ命令が利用するデータを格納する際、ＡＥＳ命令が利用する。

【００２０】

一実施形態においては、レジスタファイルは、ストリーミング（シングルインストラクションマルチプルデータ（ＳＩＭＤ））エクステンション（ＳＳＥ）インストラクションのセットを有するＩｎｔｅｌ　Ｐｅｎｔｉｕｍ（登録商標）　ＭＭＸプロセッサに提供されている１２８ビットのＭＭＸレジスタに類似した１２８ビットレジスタ群である。ＳＩＭＤプロセッサでは、データが１２８ビットブロックで処理され、一度に１つの１２８ビットブロックがロードされる。

【００２１】

フェッチ復号化部２０６は、Ｌ１命令キャッシュ２０２からマイクロインストラクションをフェッチして、該マイクロインストラクションを復号化して、マイクロコード読み取り専用メモリ（ＲＯＭ）２１４に格納されうるマイクロ演算（μｏｐｓ）と称される簡単な演算に分割する。実行部２１０は、マイクロ演算をスケジューリングして実行する。示されている実施形態では、実行部２１０のＡＥＳ機能１０３は、ＡＥＳ命令セット用のマイクロ演算を含む。リタイヤ部２１２は、実行された命令の結果を、レジスタまたはメモリに書き込む。ＡＥＳ命令が利用するラウンド鍵２１４は、Ｌ１データキャッシュ２０４に格納されており、実行部２１０にロードされて、マイクロ演算がＡＥＳ命令セットのＡＥＳ命令を実行するのに利用されてよい。ラウンド鍵２１４をデータキャッシュ２０４に格納することで、例えばシステム１００に格納されている暗号化情報にアクセスすべくラウンド鍵を取得しようとする試みのようなサイドチャネル攻撃からラウンド鍵を守る。

【００２２】

図３は、本発明の原理によりＡＥＳ暗号化および復号化を行う図２に示す実行部２１０の一実施形態を示すブロック図である。図３を、図２との関連で説明する。

【００２３】

フェッチ復号化部２０６がＡＥＳ命令を復号した後、実行部２１０はＡＥＳ命令を、マイクロコードＲＯＭ２１４に格納されていてよいＡＥＳ命令に関するマイクロ演算を行うことで実行する。

【００２４】

本発明の一実施形態による柔軟なＡＥＳ命令セットにより、プログラマーは、処理データ量、メモリ帯域幅および容量に対する性能のトレードオフを行うことができる。

【００２５】

アプリケーションによっては、同じ鍵を使い続けるものもある。性能が非常に重要なアプリケーションでは、鍵の鍵スケジュールを１度予め計算して（つまり、ラウンド毎のラウンド鍵）、それをメモリに格納しておくという観点でのトレードオフが行われる。他の種類のアプリケーションには、鍵スケジュールを格納するのに利用されるメモリ量を最小限に抑え、且つ、マルチブロック演算では良好な性能を達成することを望むものもある。この種類のアプリケーションでは、鍵スケジュールを、処理前に多数のブロックについて予め演算しておくことが考えられる。暗号鍵または逆暗号鍵のみを格納して、他のものは適宜性能面の犠牲を鑑みながら生成することによって、メモリフットプリントがさらに低減されうる。

【００２６】

ｘ８６－型プロセッサでは、ＡＥＳラウンド鍵演算およびＡＥＳスケジューリング演算が利用可能な領域および実行ポート数により、ＡＥＳ命令の性能に制限が加わる。鍵拡張が全てのブロック暗号化で必要となるシステムにおいては、ＡＥＳスケジューリング演算およびＡＥＳラウンド鍵演算を異なる実行ポートに実装することで、性能を向上させる可能性がある。しかし、ｘ－８６型プロセッサでは、異なる実行ポートおよびこれら異なるポート制御用の追加領域は提供不可能なことがある。

【００２７】

一実施形態では、暗号化ラウンド、復号化ラウンド、暗号化復号化最終ラウンド最終ラウンドを行い、ラウンド暗号鍵またはラウンド復号鍵を算出するのに、それぞれ別個のＡＥＳ命令を含むＡＥＳ命令セットが提供される。一実施形態では、ＡＥＳ命令セットが６つのＡＥＳ命令を含む。各ＡＥＳラウンド命令は、固有演算コード（ｏｐｃｏｄｅ）を有する。固定幅ラウンド鍵の一実施形態（例えば１２８ビット）におけるＡＥＳ命令セットのＡＥＳラウンド命令を、以下の表１に示す。

【表１】

AESENCRYPTRound xmmsrcdst xmm

入力: データ(=宛先)、ラウンド鍵

出力: ラウンド鍵を用いたAESラウンドによる変換後のデータ

AESENCRYPTLastRound xmmsrcdst xmm

入力: データ(=宛先)、ラウンド鍵

出力: ラウンド鍵を用いたAES最終ラウンドによる変換後のデータ

AESDECRYPTRound xmmsrcdst xmm

入力: データ(=宛先)、ラウンド鍵

出力: ラウンド鍵を用いたAESラウンドによる変換後のデータ

AESDECRYPTLastRound xmmsrcdst xmm

入力: データ(=宛先)、ラウンド鍵

出力: ラウンド鍵を用いたAES最終ラウンドによる変換後のデータ

AESNextRoundKey xmmsrc1,2 xmm dst（直近）

入力: 鍵の下位128ビット、鍵の上位128ビット、ラウンド数のインジケータ

出力: 入力から得られた次のラウンド鍵

AESPreviousRoundKey xmmsrc1,2 xmm dst（直近）

入力: 鍵の下位128ビット、鍵の上位128ビット、ラウンド数のインジケータ

出力: 入力から得られた前のラウンド鍵

【００２８】
ＡＥＳ命令セットは、４つのＡＥＳラウンド命令（暗号化、復号化、暗号化最終ラウンド、復号化最終ラウンド）、および２つのＡＥＳラウンド鍵命令（次のラウンド鍵および前のラウンド鍵）を含む。ＡＥＳ命令セットのＡＥＳラウンド命令は、最終ラウンド以外の全てのラウンドに利用される暗号化および復号化ラウンド演算を行うシングルラウンド演算を含む。例えば、表１のAESENCRYPTRoundのシングルラウンド命令では、入力データが１２８ビットレジスタ（xmmsrcdst）に格納され、ラウンド鍵が別の１２８ビットレジスタ（xmm）に格納される。この命令は、１２８ビットxmmsrcdstレジスタに格納されている入力データ（ソース）に対してＡＥＳラウンド演算を行い、１２８ビットxmmsrcdstレジスタに格納されている入力データを、ラウンド演算実行結果で上書きする。故に、xmmsrcdstは当初は入力データを、そして後には、ＡＥＳラウンド演算結果を格納する。
【００２９】
さらにＡＥＳ命令セットは、最終復号化ラウンドのＡＥＳ復号命令および最終暗号化ラウンドのＡＥＳ暗号命令を含む。例えば、表１のAESENCRYPTLastRoundのシングルラウンド命令では、入力データが１２８ビットレジスタ（xmmsrcdst）に格納され、ラウンド鍵が別の１２８ビットレジスタ（xmm）に格納される。この命令は、xmmsrcdstレジスタに格納されている入力データ（ソース）に対してＡＥＳラウンド演算を行い、xmmsrcdstレジスタに格納されている入力データを、ラウンド演算実行結果で上書きする。故に、xmmsrcdstは当初は入力データを、そして後には、ラウンド演算結果を格納する。xmmレジスタは、ラウンド演算のラウンド鍵を格納する。
【００３０】
別の実施形態では、ラウンドおよび最終ラウンド命令（例えば、AESENCRYPTRoundおよびAESENCRYPTLastRound）が、レジスタファイル３０４からではなくて、メモリ（ｍ／１２８）から入力を受け取ってよい（例えば、ＡＥＳラウンド命令は、AESENCRYPTRound xmmsrcdst m/128であってよい）。
【００３１】
ＡＥＳ命令セットの他の２つのＡＥＳ命令は、鍵のサイズ（つまり、１２８ビット、１９２ビット、または２５６ビット）に応じてＡＥＳラウンド用のラウンド鍵を生成する。これらＡＥＳラウンド鍵命令の一方は暗号化演算に利用されるラウンド鍵を生成し、他方は復号化演算に利用されるラウンド鍵を生成する。AESNextRoundKey AESPreviousRoundKey命令における直近のフィールドは、鍵のサイズを特定する｛１２８、１９２、２５６｝。
【００３２】
また別の実施形態では、直近のフィールドの代わりに、異なる鍵のサイズが、各々が固有演算コードを有する別個の命令として実装されてよい。この実施形態では、ＡＥＳラウンド鍵命令の数は、各ラウンド鍵演算（例えばAESNextRoundKey_128、AESNextRoundKey_192、およびAESNextRoundKey_256）について３つの別個の命令を含み、AESPreviousRoundKeyもまた、これらに類似した３つの命令のセットを含む。この実施形態では、命令セット内の命令の総数は、先に述べた実施形態の６つに比して、１０となっている。
【００３３】
レジスタファイル３０４は、ＡＥＳ命令セットのＡＥＳ命令が利用しうる１２８ビットレジスタを複数有する。１２８ビットレジスタは、ソースオペランド、ラウンド鍵、およびＡＥＳ命令の結果を格納しうる。第１ラウンドでは、ＡＥＳ命令は、暗号される１２８ビットの平文または復号される１２８ビットの暗号文であってよいソースオペランドを受信する。１２８ビット、１９２ビット、または２５６ビットの鍵の鍵スケジュールを生成する鍵は、レジスタファイル３０４内の複数の１２８ビットレジスタ３０８のいずれかに格納されていてよい。またラウンド鍵も、レジスタファイルの１２８ビットレジスタ３０８のいずれかに格納されてよい。全ての命令は、レジスタファイルのレジスタを利用し、さらに、後述するようにメモリから直接入力を得てよい。
【００３４】

表１に示すＡＥＳ命令セットの一実施形態を利用するソースコードの例を、以下の表２に示す。本例においては、多くのブロックに対して同じ鍵を利用する暗号化を行うアプリケーションで性能が最適化されている。このようなアプリケーションの１つに、ディスクに格納する前に全てのデータを暗号化する際に同じ鍵を利用するようなディスクのコンテンツを暗号化するのに単一の鍵を利用するものがある。本例では、ＡＥＳ－１２８暗号が行われる。

【００３５】

鍵のサイズは、１２８ビット、１９２ビット、または２５６ビットであってよい。行われるラウンドの数（ｎ）は、鍵のサイズに応じて１、１０、１２、または１４で、各ラウンド鍵は固定サイズ（１２８ビット）であってよい。ラウンド値数が１０、１２、１４の場合、ＡＥＳマイクロ演算は、１２８ビット、１９２ビット、または２５６ビットの鍵サイズに対して標準的なＡＥＳ暗号化および復号化を行ってよい。

【００３６】

多くのブロックについて同じ鍵を利用する場合、各ラウンドのラウンド鍵（鍵スケジュール）は、予め計算されてメモリ（例えばレベル１データキャッシュ２０４）に格納されているので、各ブロックの暗号化／復号化演算の前に同じ鍵スケジュールを再度計算する必要がない。

【表２】

```
RK[0] = 入力鍵

For i = 1..10

  RK [i] = AESNextRoundKey (RK[i-1])

End


STATE = 入力ブロック

STATE = STATE xor RK[0]


For i = 1..9

  STATE  = AESENCRYPTRound (STATE, RK[i])

End

STATE  = AESENCRYPTLastRound (STATE, RK[10])
```

【００３７】

１０エレメントを有するアレイ（ＲＫ）を利用して、鍵の鍵スケジュールを格納する。ＡＥＳ－１２８暗号の入力鍵を、ＲＫ［０］に格納して、９ラウンド鍵ＲＫ［０］－ＲＫ［１］を、ＡＥＳ命令セットからAESNextRoundKey命令を読み出すことで予め計算する。AESNextRoundKey命令は、現在のラウンド鍵に基づいて次のラウンドを計算する。鍵スケジュールについて予め計算されたラウンド鍵は、レベル１データキャッシュ２０４のラウンド鍵２１４に格納されてよい。

【００３８】

本例においては、そのラウンドのラウンド鍵である鍵スケジュールの該当部分（拡張鍵）が直接レジスタファイル３０４から入力されると、ＡＥＳラウンドを行うループに入る前に、排他的論理和（ＸＯＲ）演算を、状態と鍵とに対して行う。各ラウンド１から９においては、ＡＥＳ命令セットからAESENCRYPTRound命令を呼び出して、ＡＥＳラウンド演算を１ラウンドについて行う。最終ラウンド（ラウンド１０）については、ＡＥＳ命令セットからAESENCRYPTLastRound命令を呼び出して、この最終ラウンドにＡＥＳラウンド演算を行う。

【００３９】

ＡＥＳ命令が暗号化または復号化する情報は、暗号または複号演算を開始する第１のＡＥＳ命令が発行される前に、レジスタファイル３０４のソース／宛先レジスタ３０６へロードされる。ソースレジスタ３０６の情報の暗号化／復号化に利用される鍵は、レジスタファイル３０４の１以上の他のレジスタ３０８に格納されている。１２８ビット鍵の場合、鍵の全１２８ビットが、レジスタファイル３０４の他の１２８ビットレジスタのいずれかに格納される。１２８ビットより大きい鍵のサイズに対しては、最上位ビット（１２８ビットより大きい）を、１２８ビットレジスタのうち別のものに格納する。

【００４０】

表２に示す例においては、レジスタファイル３０４のレジスタ３０８のいずれかにロードされる前に、鍵に基づいて各ラウンドのラウンド鍵が予め計算されて、レベル１データキャッシュ２０４に格納されていてよい。各ラウンドの鍵は、さらに、レジスタファイル３０４の１以上のレジスタに格納されていてもよく、または、レベル１データキャッシュ２０４のラウンド鍵２１４に格納されていてもよい。

【００４１】

ＡＥＳは、１２８ビットの固定ブロックサイズと、１２８、１９２、または２５６ビットの鍵サイズとを有し、４ｘ４バイトアレイ（つまり１６バイト（１２８ビット固定ブロックサイズ））で動作する（これを「状態」と称する）。ＡＥＳアルゴリズムは、１２８ビットの平文ブロックを、１２８ビットの暗号文ブロックに変換（暗号化）する、または、１２８ビットの暗号文ブロックを、１２８ビットの平文ブロックに変換（復号化）し、これらは、１０、１２、または１４の連続したラウンドで行われ、このラウンド数は鍵のサイズに応じている（１２８、１９２、または２５６ビット）。

【００４２】

ラウンド毎の暗号化または復号化演算を行う前に、実行部２１０は、状態および鍵をレジスタファイル３０４から取得する。各暗号化／復号化ラウンド演算は、読み取り専用メモリ（ＲＯＭ）２１４の鍵スケジューラ３０２に格納されているＡＥＳ命令のマイクロ演算を利用して行われる。ここに示す実施形態では、状態（１２８ビットブロックの状態）は、レジスタ３０６に格納されており、鍵は、レジスタファイル３０４の他のレジスタ３０８の１以上に格納されている。ＡＥＳ命令の実行の結果生じる状態をレジスタファイル３０４のレジスタ３０６に格納する。状態は、次のＡＥＳラウンドまたはＡＥＳ暗号化または復号化演算の最終結果が利用する中間ラウンドデータであってよい。

【００４３】

ここで示す実施形態においては、鍵スケジューラ３０２は、ＡＥＳラウンドで利用するラウンド鍵を生成する。鍵スケジューラ３０２は、マイクロコード演算として実装されてよく、ＦＩＰＳ　ＰＵＢ１９７で定義される１２８ビット、１９６ビット、および２５６ビット鍵のラウンド鍵を生成する一連の演算を行うマイクロコード演算を含みうる。

【００４４】
別の実施形態では、鍵スケジューラは、実行部２１０のハードウェア状態マシン列として実装されてよい。また別の実施形態では、鍵スケジューラの幾らかの部分がマイクロコードＲＯＭ２１４に格納されているマイクロコード演算として実装され、鍵スケジューラの残りの部分が実行部２１０のハードウェア状態マシン列として実装されてもよい。
【００４５】
鍵スケジューラ３０２は、ｎバイトの鍵を、ｂバイトの拡張鍵（鍵スケジュール）に拡張してよく、この拡張鍵の最初のｎバイトが元の鍵であってよい。例えば、１２８ビットの鍵においては、１２８ビットの鍵を１７６バイト（つまり、１１ｘ１６バイト（１２８ビット））の拡張鍵に拡張して、この最初の１６バイトが元の１２８ビットの鍵であり、ラウンド数は１０である。１９２ビットの鍵の２４バイトを、２０８バイト（１３ｘ１６バイト）に拡張して、１２個の「ラウンド鍵」を、１２ラウンドそれぞれに対して１つずつ割り当てるよう提供し、２５６ビットの鍵の３２バイトを、２４０バイト（１５ｘ１６バイト）に拡張して、１４個の「ラウンド鍵」を、１４ラウンドそれぞれに対して１つずつ割り当てるよう提供する。
【００４６】
演算コード（ｏｐｃｏｄｅ）をＡＥＳ命令で複号する際、１回のＡＥＳラウンドのＡＥＳ命令のフローを制御するのに利用されるパラメータ数は、制御ロジック３２２に格納されている。パラメータは、演算の種類（暗号または復号）およびそれが最終ラウンドであるかの情報を含む。
【００４７】
ＡＥＳラウンドロジック３２４は、ブロック状態３１４、Ｓ－ボックス／逆Ｓ－ボックス３１６、行シフト３１６および逆列混合またはヌル混合（mix inverse, mix columns or null）（「列混合」と称される）３２０、およびラウンド鍵加算３２６という段階のマイクロ演算を含みうる。
【００４８】
ブロック状態３１４では、ＡＥＳラウンドロジック３２４への１２８ビットの入力（状態）に、ビットワイズＸＯＲを用いて、鍵（ラウンドに関連付けられた拡張鍵の１２８ビットの部分）を追加して、１２８ビットの中間値（状態）を生成する。
【００４９】
Ｓ－ボックス／逆Ｓ－ボックス３１６では、この１２８ビットの中間値の各バイトを、これも置換ボックスまたは「Ｓ－ボックス」と称されるルックアップテーブルから格納・取得されうる別のバイト値で置換してよい。Ｓ－ボックスは、幾らかの数の入力ビットｍを取り、それらを幾らかの数の出力ビットｎに変換して、通常ルックアップテーブルとして実装する。固定ルックアップテーブルが通常利用される。この演算は、ガロア体（ＧＦ）（2^8）において逆関数を利用することで非線形性を生じる。例えば、ｎビットの出力は、ｍビットの入力の外側の２ビットを用いてルックアップテーブルで行を選択し、ｍビットの入力の内側のビットを用いて列を選択することで、見つけることができる。
【００５０】
行シフト３１８ではＳ－ボックス／逆Ｓ－ボックス３１６の結果に、ビット線形変換を行い、サブバイト段階から受け取った４ｘ４アレイ（１２８ビット（１６バイト）状態）の各行のバイトを、周期的に左にシフトさせる。各バイトをシフトさせる位置の数は、４ｘ４アレイの各行によって異なる。
【００５１】
列混合３２０では、行シフト３１８の結果に、ビット線形変換を行い、４ｘ４アレイ（状態）の各行を、バイナリガロア体（ＧＦ）（2^8）上の多項式として扱い、その後、ｃ（ｘ）＝$3x^3+x^2+x+2$を固定多項式として、モジュロx^4+1乗算する。最終ＡＥＳラウンドは、他のＡＥＳラウンドと、列混合３２０が省かれている点で異なっている。
【００５２】

列混合段階３２０の後、ラウンド鍵加算３２４では、拡張鍵からのラウンド鍵、およびそのＡＥＳラウンドの行シフト３１８または列混合３２０の結果の排他的論理和演算を行う。

【００５３】

例えば、以下のＡＥＳ命令を発行して、ＡＥＳ復号の１ラウンドを行うことができる。

AESDECRYPTRound xmmsrcdst xmm

【００５４】

本例では、１２８ビットＡＥＳ暗号化ラウンド演算を、拡張鍵が{ＲＫ［１］，ＲＫ［２］，…ＲＫ［１０］}として表される鍵を利用して行う。ラウンド鍵は、AESDECRYPTRound命令を発行する前に、AESPreviousRoundKey xmmsrc1,2 xmm dst（中間）命令を発行することで生成されうる。ラウンド鍵は、レベル１データキャッシュ２０４からブロック状態３１４へ直接ロードされてもよいし、または、先ずレジスタファイル３０４のレジスタ（xmm）に格納されていて、その後、レジスタからブロック状態３１４へロードされてもよい。

【００５５】

異なる鍵を利用して各ブロックを暗号化／復号化する場合（例えば、データパケットを暗号化／復号化するネットワークインタフェースコントローラ（ＮＩＣ）の場合）、ラウンド鍵は、以下の表３でＡＥＳ－１２８暗号の疑似コードで示すように各ラウンドについて暗号化／復号化を行う前に、その都度計算されてよい。

【表３】

```
RK[0] = 入力鍵

STATE = 入力ブロック
STATE = STATE xor RK[0]

For i = 1..9
  RK [i] = AESNextRoundKey (RK[i-1])
  STATE  = AESENCRYPTRound (STATE, RK[i])
End
RK [10] = AESNextRoundKey (RK[9])
STATE  = AESENCRYPTLastRound (STATE, RK[10])
```

【００５６】

本例においては、該ラウンドのラウンド鍵は、鍵スケジュール（拡張鍵）の１０ラウンド各々（つまり、ラウンド１－９およびラウンド１０（最終ラウンド））に対してラウンド鍵を利用して暗号化を行う前に生成される。

【００５７】

シングルＡＥＳラウンド命令およびシングルＡＥＳラウンド鍵生成命令を含むＡＥＳ命令セットにより、異なる数のラウンドおよび鍵スケジュールを有するＡＥＳの変形例を生成することができる、つまり、ＦＩＰＳ　ＰＵＢ１９７では定義されていないＡＥＳの変形例を生成することができる。故に、ＡＥＳ命令セットのシングルラウンドＡＥＳ命令は、ＡＥＳ暗号化および復号化を行う際に柔軟性を提供する。

【００５８】
ＡＥＳ命令セットが行うラウンド数は固定されていないので、適宜任意の数のラウンドを行うことができる。例えば、ラウンド数は、ハッシュまたはＭＡＣ攻撃またはＡＥＳへの攻撃に対する新たな規格が導入された場合、将来の暗号化／復号化規格をサポートするよう変更可能である。
【００５９】
図４は、図３の実行部２１０によるＡＥＳ暗号化ラウンド命令のフローを示すフローグラフである。
【００６０】
ブロック４００で、実行部２１０は、ＡＥＳ暗号化ラウンド命令を待つ。ＡＥＳ暗号化ラウンド命令がフェッチ復号化部２０６により既に復号化されている場合、処理はブロック４０２に進む。復号化されていない場合は、ブロック４００に留まり、ＡＥＳ暗号化ラウンド命令を待つ。
【００６１】
ブロック４０２で、フェッチ復号化部２０６による命令復号化中、暗号化が必要である旨を制御ロジック３２２に格納して、暗号化ラウンド実行に利用されるラウンド鍵および１２８ビットブロック状態（ソース）をレジスタファイル３０４から実行部２１０へロードする。処理はブロック４０４へ進む。
【００６２】
ブロック４０４で、置換演算を１２８ビットブロック状態に対して、つまり、ブロック４０６または４１８の結果に対して、行う。１２８ビットブロック状態の各バイトを、これも置換ボックスまたは「Ｓ－ボックス」と称されるルックアップテーブルから格納・取得されうる別のバイト値で置換してよい。Ｓ－ボックスは、幾らかの数の入力ビットｍを取り、それらを幾らかの数の出力ビットｎに変換して、通常ルックアップテーブルとして実装する。結果を、１２８ビットブロック状態として格納する。処理はブロック４０６へ進む。
【００６３】
ブロック４０６で、１２８ビットブロック状態（４ｘ４アレイ）に、ビット線形変換を行い、４ｘ４アレイの各行のバイトを、周期的に左にシフトさせる。各バイトをシフトさせる位置の数は、４ｘ４アレイの各行によって異なる。処理はブロック４０８へ進む。
【００６４】
ブロック４０８で、１２８ビットブロック状態（４ｘ４アレイ）に、ビット線形変換を行い、４ｘ４アレイ（状態）の各行を、ＧＦ（2^8）により多項式として扱い、その後、ｃ（ｘ）＝$3x^3+x^2+x+2$を固定多項式として、モジュロx^4+1乗算する。処理はブロック４１０へ進む。
【００６５】
ブロック４１０で、拡張鍵からのラウンド鍵、およびそのＡＥＳラウンドの行シフト３１８または列混合３２０の結果の排他的論理和演算を行う。処理はブロック４１２へ進む。
【００６６】
ブロック４１２で、そのラウンドの暗号化演算の結果（１２８ビットブロック状態）を、レジスタファイル３０４のソース／宛先レジスタ３０２に格納する。これでＡＥＳ暗号化命令処理が完了する。
【００６７】
以下の表４は、表３に示す疑似コードの実行後に、１２８ビットブロック入力に１２８ビット鍵を利用してＡＥＳ－１２８暗号化を行った結果の一例を示す。

【表４】

128ビット入力： 00112233445566778899aabbccddeeff (Hexadecimal)

128ビット鍵： 000102030405060708090a0b0c0d0e0f (Hexadecimal)

128ビット結果： 69c4e0d86a7b0430d8cdb78070b4c55a (Hexadecimal)

【００６８】

図５は、図３の実行部２１０によるＡＥＳ暗号化最終ラウンド命令のフローを示すフローグラフである。

ブロック５００で、実行は、ＡＥＳ暗号化最終ラウンド命令を待つ。もしもＡＥＳ暗号化最終ラウンド命令がフェッチ復号化部２０６で既に復号化されている場合、処理はブロック５０２に進む。復号化されていない場合は、ブロック５００に留まり、ＡＥＳラウンド暗号化命令を待つ。

ブロック５０２で、ブロック４０４（図４）との関連で説明したＳ－ボックスルックアップに類似した方法で最終ラウンドにＳ－ボックスルックアップを行う。処理はブロック５０４へ進む。

ブロック５０４で、ブロック４０６（図４）で他のラウンドとの関連で説明したような方法で最終ラウンドに行シフト演算を行う。処理はブロック５０６へ進む。

ブロック５０６で、拡張鍵からのラウンド鍵、およびそのＡＥＳラウンドの行シフト３１８または列混合３２０の結果の排他的論理和演算を行う。処理はブロック５０８へ進む。

ブロック５０８で、暗号化最終ラウンド演算の結果を、レジスタファイル３０４のソース／宛先レジスタ３０６に格納する。これでＡＥＳ命令の処理が完了する。

【００６９】

図６は、図３の実行部２１０によるＡＥＳ復号化ラウンド命令のフローを示すフローグラフである。

ブロック６００で、実行は、ＡＥＳ復号化ラウンド命令を待つ。ＡＥＳ復号化ラウンド命令がフェッチ復号化部２０６により既に復号化されている場合、処理はブロック６０２に進む。復号化されていない場合は、ブロック６００に留まり、ＡＥＳ復号化ラウンド命令を待つ。

ブロック６０２で、フェッチ復号化部２０６による命令復号化中、復号化ラウンドを行う必要がある旨を制御ロジック３２２に格納して、復号化ラウンド実行に利用されるラウンド鍵およびソース（１２８ビットブロック状態）をレジスタファイル３０４から実行部２１０へロードする。処理はブロック６０４へ進む。

ブロック６０４で行う処理は復号化である。ＡＥＳ規格に定義されている逆ｓ－ボックスルックアップを行うことで、置換演算を１２８ビットブロック状態に対して行う。処理はブロック６０６へ進む。

ブロック６０６で、ＦＩＰＳ　ＰＵＢ１９７で定義されている逆行シフト演算を行う。処理はブロック６０８へ進む。

ブロック６０８で、ＦＩＰＳ　ＰＵＢ１９７で定義されている逆行シフト演算を行う。処理はブロック６１０へ進む。

ブロック６１０で、拡張鍵からのラウンド鍵、およびそのＡＥＳラウンドの行シフト３１８または列混合３２０の結果の排他的論理和演算を行う。処理はブロック６１２へ進む。

ブロック６１２で、そのラウンドの復号化演算の結果（１２８ビットブロック状態）を、レジスタファイル３０４のソース／宛先レジスタ３０２に格納する。これでＡＥＳ復号化ラウンド命令処理が完了する。

【００７０】

図７は、図３の実行部２１０によるＡＥＳ復号化最終ラウンド命令のフローを示すフローグラフである。

ブロック７００で、実行部２１０は、ＡＥＳ復号化最終ラウンド命令を待つ。もしもＡＥＳ復号化最終ラウンド命令がフェッチ復号化部２０６で既に復号化されている場合、処理はブロック７０２に進む。復号化されていない場合は、ブロック７００に留まり、ＡＥＳ復号化ラウンド命令を待つ。

ブロック７０２で、ＦＩＰＳ　ＰＵＢ１９７で定義されている逆ｓ－ボックスルックアップを行うことで、最終ラウンドの１２８ビットブロック状態に置換演算を行う。処理はブロック７０４へ進む。

ブロック７０４で、ＦＩＰＳ　ＰＵＢ１９７で定義されているような方法で最終ラウンドに逆行シフト演算を行う。処理はブロック７０６へ進む。

ブロック７０６で、拡張鍵からのラウンド鍵、およびそのＡＥＳラウンドの行シフト３１８または列混合３２０の結果の排他的論理和演算を行う。処理はブロック７０８へ進む。

ブロック７０８で、復号化最終ラウンド演算の結果を、レジスタファイル３０４のソース／宛先レジスタ３０６に格納する。これでＡＥＳ復号化最終ラウンド命令の処理が完了する。

【００７１】

一実施形態では、図４－７のフローグラフのブロックを、実行部２１０のハードウェア状態マシン列として実装することができる。別の実施形態では、ブロックの幾らかの部分が読み取り専用メモリ（ＲＯＭ）２１４に格納されうるマイクロプログラムとして実装することもできる。ブロックがハードウェア状態マシン列として実装されている実施形態のほうが性能は高いと考えられる。

【００７２】

図８は、ラウンド鍵を生成し暗号化および復号化を行うのに利用されうる直近のバイトを有するＡＥＳラウンド命令の一実施形態を示す。表１に示すＡＥＳ命令セットの代わりに単一のＡＥＳラウンド命令を提供することで、ＡＥＳ命令セットの機能を行う。単一のＡＥＳ命令が行う特定の機能は、直近のバイト（key_select_modifier）内のビットに暗号化されている。直近のバイトにより、ＡＥＳラウンド命令は、各命令が固有演算コードを有する複数の新たな命令を作成する代わりに、新たな特徴を追加するよう拡張される。

【００７３】

ＡＥＳラウンド命令は、記号として以下のように定義されうる。

dest:=aes_key_round(source2,source1),key_select_modifier

【００７４】

aes_key_round命令はＡＥＳ暗号または復号化演算を行うべく、ポート番号に基づいて特定の実行部２１０に発行される。示されている実施形態では、ポート番号４がＡＥＳラウンド命令に指定された実行ポートである。実行部２１０は、多くのパラレルポート（スーパーースカラー）に分割される。しかし、全てのポートが等しいわけではない。ポートの中には、大きな整数のマルチプライアー、浮動小数点のマルチプライアーまたはデバイダ等の専用リソースを有するものがある。加算、減算、および排他的論理和等の、これらより簡単で一般的な命令は、多数のポートによりサポートされて最大の性能を発揮する。故に、各命令またはマイクロ演算では、発行制御ロジックがマイクロ演算／命令を発行するポートを決定する。本実施形態では、ＡＥＳ命令は常にポート番号４に対して発行される。しかし、他の実施形態では他のポート番号を利用することができる。

【００７５】

図８を参照すると、destはラウンドＮに対して１２８ビットの拡張鍵を格納し、ソース２はラウンドＮ－１に対して１２８ビットの拡張鍵を格納し、ソース１はラウンドＮ－２に対して１２８ビットの拡張鍵を格納する。key_select_modifierは、現在のラウンド数（Ｎ）、演算の方向（暗号化／復号化）、およびＡＥＳ鍵のサイズを提供するのに利用される８ビットの直近の値である。ＡＥＳ－１２８では、ソース１は不要であるので無視される。実行部はＡＥＳ部であり、フラグ（整数または浮動小数点）は利用されない。

【００７６】

一実施形態では、直近の値の４つの最下位ビットのビット暗号化は、ＡＥＳ－１２８に対して１－１０のラウンド数、ＡＥＳ－１９２に対して１－１２のラウンド数、およびＡＥＳ－２５６に対して２－１４のラウンド数、といったラウンド数を示す。ＡＥＳ１２８および１９２では、ラウンド数０は無効である、というのも、最初のラウンドが無変更の入力鍵を利用するからである。ＡＥＳ－２５６では、ラウンド数０と１は無効である、というのも、最初の２つの１２８ビットラウンドが無変更の２５６ビット入力鍵を利用するからである。

【００７７】

直近のバイトのビット４は演算の方向（暗号化または復号化）を示す（例えば一実施形態では０＝暗号、および１＝復号、また別の実施形態では１＝暗号、および０＝復号、というように）。直近のバイトのビット５および６は、ＡＥＳ鍵のサイズを示す。一実施形態では、ＡＥＳ鍵のサイズは以下の表５に示すように定義される。

【表５】

ビット[6:5]	鍵のサイズ
00	128
01	192
10	256
11	リザーブ

【００７８】

別の実施形態では、値１１を有するビット［６：５］も、１２８ビットの鍵のサイズのインジケータである。この実施形態では、ビット［６：５］の全ての値が有効であり、パースされうる。

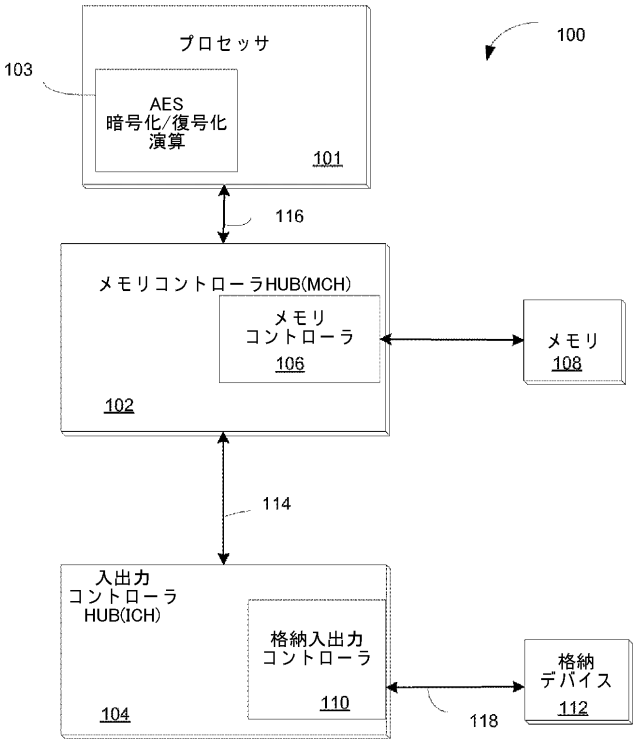
【００７９】

当業者であれば、本発明の実施形態に係る方法を、コンピュータ利用可能な媒体を含むコンピュータプログラムプロダクトに具現化することができることを想到しよう。例えば、コンピュータ利用可能な媒体は、コンピュータ可読プログラムコードが記憶されたコンパクトディスク読み取り専用メモリ（ＣＤ　ＲＯＭ）ディスクまたは従来のＲＯＭデバイス、またはコンピュータディスク等の読み取り専用メモリデバイスから形成されてよい。

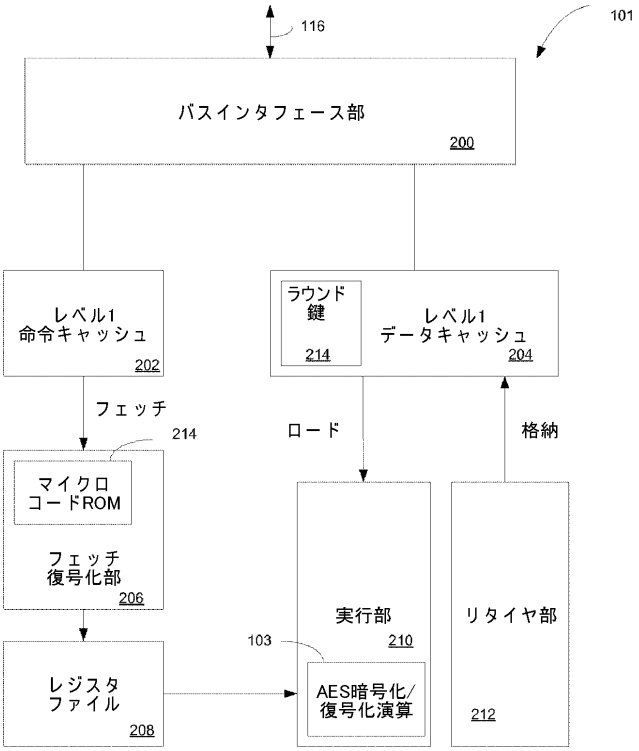
【００８０】

本発明の実施形態を特別に示し、実施形態を参照しながら記載してきたが、当業者であれば添付請求項が包括する本発明の実施形態の範囲を逸脱することなく、様々な変更を形態および詳細に対して加えることが可能であることを理解しよう。

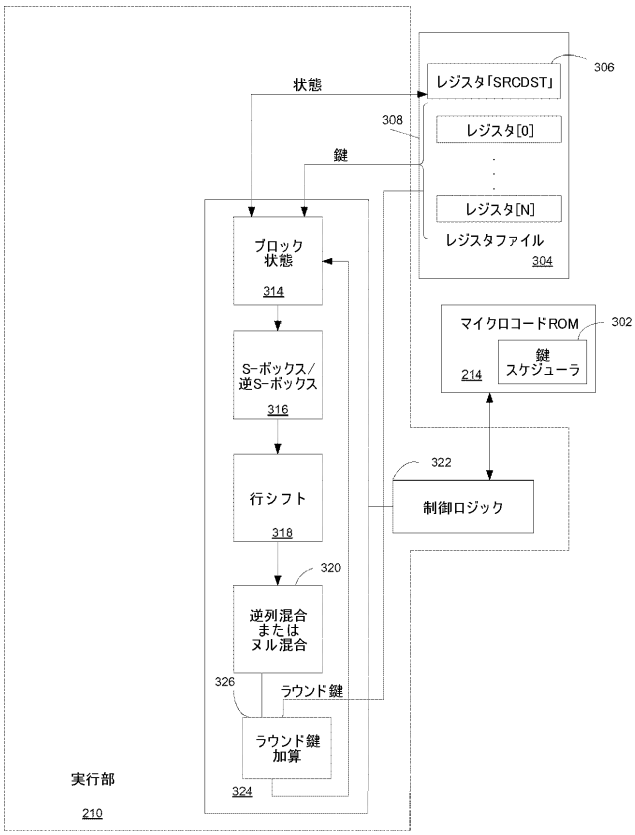
【図１】


プロセッサ
AES
暗号化/復号化
演算
101
103
100
116
メモリコントローラHUB(MCH)
メモリ
コントローラ
106
102
メモリ
108
114
入出力
コントローラ
HUB(ICH)
格納入出力
コントローラ
110
104
格納
デバイス
112
118

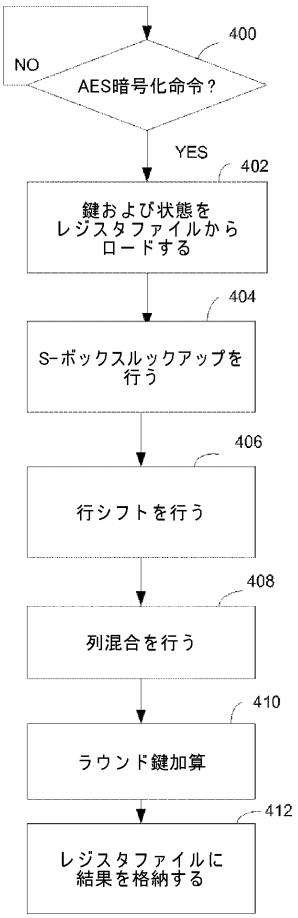
【図２】


116
101
バスインタフェース部
200
レベル1
命令キャッシュ
202
ラウンド
鍵
214
レベル1
データキャッシュ
204
フェッチ
214
ロード
格納
マイクロ
コードROM
フェッチ
復号化部
206
実行部
210
103
リタイヤ部
レジスタ
ファイル
208
AES暗号化/
復号化演算
212

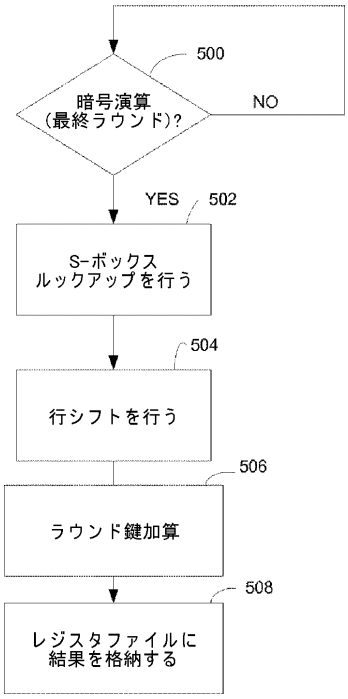
【図３】


状態
鍵
306
レジスタ「SRCDST」
308
レジスタ[0]
レジスタ[N]
レジスタファイル
304
ブロック
状態
314
S-ボックス/
逆S-ボックス
316
行シフト
318
320
逆列混合
または
ヌル混合
326
ラウンド鍵
ラウンド鍵
加算
324
実行部
210
マイクロコードROM
302
214
鍵
スケジューラ
322
制御ロジック

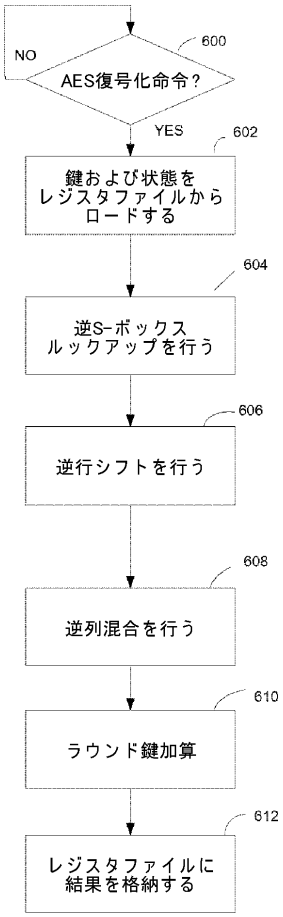
【図４】


400
NO
AES暗号化命令？
YES
402
鍵および状態を
レジスタファイルから
ロードする
404
S-ボックスルックアップを
行う
406
行シフトを行う
408
列混合を行う
410
ラウンド鍵加算
412
レジスタファイルに
結果を格納する

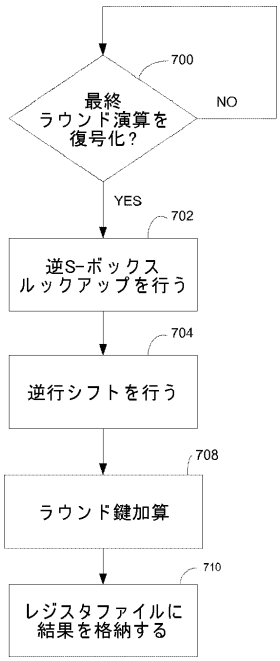
【図５】



【図６】



【図７】



【図８】

dest:= aes_key_round(source2, source1), key_select_modifier

ポート						整数フラグ						浮動小数点フラグ				
0	1	2	3	4	5	O	S	Z	A	P	C	PreC	C3	C2	C1	C0
-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-

実行部	AES部
整数イベント	-
前処理イベント	N/A
後処理イベント	N/A

【手続補正書】
【提出日】平成21年9月3日(2009.9.3)
【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命令の一連の演算を行う実行部を備える装置であって、
前記一連の演算は、プラグラム可能な数のＡＥＳラウンドを行い、
前記演算は前記実行部に、
前記ＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードさせ、
各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成させ、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行わせて、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供させる、装置。
【請求項２】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記実行部は、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする、請求項１に記載の装置。
【請求項３】
前記一連のＡＥＳラウンド演算により、前記実行部は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成し、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行い、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う、請求項２に記載の装置。
【請求項４】
前記ＡＥＳラウンドの数－１に対して前記一連のＡＥＳラウンド演算を行うことで、前記実行部は、
前記ＡＥＳラウンドの前記入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成し、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行い、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行い、
前記置換演算の結果に、前記中間値の列同士を混合させるビット線形変換を行う、請求項１に記載の装置。
【請求項５】
最終ラウンドに前記一連のＡＥＳラウンド演算を行うことで、前記実行部は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成し、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行い、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う、請求項４に記載の装置。
【請求項６】
前記結果は暗号化された値である、請求項１に記載の装置。

【請求項７】
前記結果は復号化された値である、請求項１に記載の装置。
【請求項８】
第１のＡＥＳラウンドの鍵および入力がレジスタファイルに格納されている、請求項１に記載の装置。
【請求項９】
前記レジスタファイルは複数の１２８ビットレジスタを含む、請求項８に記載の装置。
【請求項１０】
ＡＥＳ命令のプログラム可能なＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードして、各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成する段階と、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行い、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供する段階と、を備える方法。
【請求項１１】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする段階を備える、請求項１０に記載の方法。
【請求項１２】
前記一連のＡＥＳラウンド演算を行う段階は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成する段階と、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行う段階と、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う段階と、を有する、請求項１１に記載の方法。
【請求項１３】
前記ラウンドの数１に対して前記一連のＡＥＳラウンド演算を行う段階は、
前記ＡＥＳラウンドの前記入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成する段階と、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行う段階と、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う段階と、
前記置換演算の結果に、前記中間値の列同士を混合させるビット線形変換を行う段階と、を有する、請求項１０に記載の方法。
【請求項１４】
最終ＡＥＳラウンドに前記一連のＡＥＳラウンド演算を行う段階は、
前記ラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して排他的論理和（ＸＯＲ）演算を行って、中間値を生成する段階と、
ルックアップテーブルに格納されている値に基づいて、前記中間値の各バイトに対して置換演算を行う段階と、
前記置換演算の結果に、前記中間値の行をシフトさせるビット線形変換を行う段階と、を有する、請求項１３に記載の方法。
【請求項１５】
前記結果は暗号化された値である、請求項１０に記載の方法。
【請求項１６】
前記結果は復号化された値である、請求項１０に記載の方法。
【請求項１７】
第１のＡＥＳラウンドの鍵および入力がレジスタファイルに格納されている、請求項１０に記載の方法。

【請求項１８】
前記レジスタファイルは複数の１２８ビットレジスタを含む、請求項１７に記載の方法。
【請求項１９】
コンピュータに、
ＡＥＳ命令のプログラム可能なＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードし、各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成する手順と、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行わせて、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供する手順と、を実行させるためのプログラム。
【請求項２０】
コンピュータに、
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする手順、をさらに実行させるための請求項１９に記載のプログラム。
【請求項２１】
データおよび命令を格納するダイナミックランダムアクセスメモリと、
前記メモリに連結されて前記命令を実行するプロセッサと、を備えるシステムであって、
前記プロセッサは、
ＡＥＳ命令の一連の演算を行う実行部を備え、
前記一連の演算は、プラグラム可能な数のＡＥＳラウンドを行い、
前記演算は前記実行部に、
前記ＡＥＳラウンドの数が１より大きい場合、鍵を一時的鍵レジスタにロードさせ、
各ＡＥＳラウンドを行う前に、前記鍵に基づいて前記ＡＥＳラウンドのラウンド鍵を生成させ、
各ＡＥＳラウンドにおいて、前記ＡＥＳラウンドの入力および前記ＡＥＳラウンドの前記ラウンド鍵に対して一連のＡＥＳラウンド演算を行わせて、次のＡＥＳラウンドの次の入力または前記ＡＥＳ命令の結果を提供させる、システム。
【請求項２２】
前記ＡＥＳラウンドの数が１に等しい場合、前記一連のＡＥＳラウンド演算を行う前に、前記実行部は、前記鍵に基づいて前記ＡＥＳラウンドについて予め計算されたラウンド鍵をロードする、請求項２１に記載のシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/058128

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/10(2006.01)i, H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : H04L 9/00, H04L 9/18, H04K 1/04, G06F 9/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility Models and applicaitons for Utility Model since 1975
Japanese Utility Models and applicaitons for Utility Model since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal), IEEE xpl, Google, "modification", "aes", "encryiption", "round key"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/0108195 A1 (Fujitsu limited, Kawasaki) 12 Jun 2003. See the whole document	1-22
X	US 2005/0213756 A1 (Koninklijke philips Electronics N.V.) 29 Sep 2005. see abstract, fig.1-5 and claims 1-52	1-22
Y	WO 03/019357 A1 (INFINEON THECHNOLOGIES AG) 6 March 2003. see abstract, fig.1-2	1-22
Y	KR 10-2002-0061718 A (LG Electronics Co. Ltd.) 17 Jan 2001. see abstract, fig 2.	1-22

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 JULY 2008 (31.07.2008)	**31 JULY 2008 (31.07.2008)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	MA, Jung Youn Telephone No. 82-42-481-5679

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2008/058128

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 20030108195 A1	12.06.2003	EP 1271839 B1	22.09.2004
		JP 15015522 A	17.01.2003
		DE 60105788 T2	10.02.2005
US 20050213756 A1	29.09.2005	AU 2003239730 AA	06.01.2004
		EP 1518347 A2	30.03.2005
		JP 2005531023 T2	13.10.2005
		US 2005133902 A1	23.06.2005
		WO 2004002057 A3	21.05.2004
WO 2003019357 A1	06.03.2003	EP 1419436 A1	19.05.2004
KR 2002061718 A	25.07.2002	US 20020131588 A1	19.09.2002

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 フェガリ、ワジ、ケー.
アメリカ合衆国 ９５０５２ カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・２２００ インテル・コーポレーション内
(72)発明者 ゴーパル、ヴィノード
アメリカ合衆国 ９５０５２ カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・２２００ インテル・コーポレーション内
(72)発明者 ラグナンダン、マカラム
アメリカ合衆国 ９５０５２ カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・２２００ インテル・コーポレーション内
(72)発明者 ディクソン、マーティン、ジー.
アメリカ合衆国 ９５０５２ カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・２２００ インテル・コーポレーション内
(72)発明者 チェヌパティ、スリニヴァス
アメリカ合衆国 ９５０５２ カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・２２００ インテル・コーポレーション内
(72)発明者 クーナヴィス、マイケル、イー.
アメリカ合衆国 ９５０５２ カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・２２００ インテル・コーポレーション内

Ｆターム(参考) 5J104 AA32 JA07 NA02 NA09 NA10 NA37