(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5197258号
(P5197258)
(45)発行日　平成25年5月15日(2013.5.15)　(24)登録日　平成25年2月15日(2013.2.15)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 610A

請求項の数 12 (全 72 頁)

(21)出願番号　特願2008-233094(P2008-233094)
(22)出願日　平成20年9月11日(2008.9.11)
(65)公開番号　特開2009-109988(P2009-109988A)
(43)公開日　平成21年5月21日(2009.5.21)
審査請求日　平成23年9月2日(2011.9.2)
(31)優先権主張番号　特願2007-264967(P2007-264967)
(32)優先日　平成19年10月10日(2007.10.10)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】暗号処理回路

(57)【特許請求の範囲】
【請求項１】
AESの暗号処理回路であって、
第１のAddRoundKey演算部と第２のAddRoundKey演算部とShiftRows演算部とSubBytes演算部とMixColumns演算部とデータ保持部を有し、
前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と前記ShiftRows演算部と前記SubBytes演算部と前記MixColumns演算部と前記データ保持部を用いて、複数のクロックサイクルで暗号化処理を行い、
前記暗号化処理の最後のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部を用い、かつ、前記MixColumns演算部を用いず、
前記最後のクロックサイクルを除く、前記暗号化処理のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部のうち、いずれか１つのAddRoundKey演算部を用いることを特徴とする暗号処理回路。
【請求項２】
前記暗号化処理の最初のクロックサイクルでは、平文データを前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記SubBytes演算部に入力し、前記SubBytes演算部の出力を前記ShiftRows演算部に入力し、前記ShiftRows演算部の出力を前記MixColumns演算部に入力し、前記MixColumns演算部の出力を前記データ保持部に入力し、
前記暗号化処理の２クロックサイクル目からラウンド数Nr-1クロックサイクル目では、

前記データ保持部の出力を前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記SubBytes演算部に入力し、前記SubBytes演算部の出力を前記ShiftRows演算部に入力し、前記ShiftRows演算部の出力を前記MixColumns演算部に入力し、前記MixColumns演算部の出力を前記データ保持部に入力し、

前記暗号化処理のラウンド数Nrクロックサイクル目では、前記データ保持部の出力を前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記SubBytes演算部に入力し、前記SubBytes演算部の出力を前記ShiftRows演算部に入力し、前記ShiftRows演算部の出力を前記第2のAddRoundKey演算部に入力し、前記第2のAddRoundKey演算部の出力を前記データ保持部に入力することを特徴とする請求項１に記載の暗号処理回路。

【請求項３】

CipherKeyからRoundKeyを生成し、前記生成したRoundKeyを前記第１のAddRoundKey演算部及び前記第２のAddRoundKey演算部に供給するための鍵拡張部と、

前記暗号化処理の開始からのクロックサイクルをカウントし、前記暗号化処理を行うための制御信号を生成する制御部を有することを特徴とする請求項１又は２に記載の暗号処理回路。

【請求項４】

AESの暗号処理回路であって、

第１のAddRoundKey演算部と第２のAddRoundKey演算部とInvShiftRows演算部とInvSubBytes演算部とInvMixColumns演算部とデータ保持部を有し、

前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と前記InvShiftRows演算部と前記InvSubBytes演算部と前記InvMixColumns演算部と前記データ保持部を用いて、複数のクロックサイクルで復号処理を行い、

前記復号処理の最初のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部を用い、かつ、前記InvMixColumns演算部を用いず、

前記最初のクロックサイクルを除く、前記復号処理のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部のうち、いずれか一方のAddRoundKey演算部を用いることを特徴とする暗号処理回路。

【請求項５】

前記復号処理の最初のクロックサイクルでは、暗号文データを前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記InvShiftRows演算部に入力し、前記InvShiftRows演算部の出力を前記InvSubBytes演算部に入力し、前記InvSubBytes演算部の出力を前記第2のAddRoundKey演算部に入力し、前記第2のAddRoundKey演算部の出力を前記データ保持部に入力し、

前記復号処理の２クロックサイクル目からラウンド数Nr-1クロックサイクル目では、前記データ保持部の出力を前記InvMixColumns演算部に入力し、前記InvMixColumns演算部の出力を前記InvShiftRows演算部に入力し、前記InvShiftRows演算部の出力を前記InvSubBytes演算部に入力し、前記InvSubBytes演算部の出力を前記第2のAddRoundKey演算部に入力し、前記第2のAddRoundKey演算部の出力を前記データ保持部に入力し、

前記復号処理のラウンド数Nrクロックサイクル目では、前記データ保持部の出力を前記InvMixColumns演算部に入力し、前記InvMixColumns演算部の出力を前記InvShiftRows演算部に入力し、前記InvShiftRows演算部の出力を前記InvSubBytes演算部に入力し、前記InvSubBytes演算部の出力を前記第2のAddRoundKey演算部に入力し、前記第2のAddRoundKey演算部の出力を前記データ保持部に入力することを特徴とする請求項４に記載の暗号処理回路。

【請求項６】

CipherKeyからRoundKeyを生成し、前記第１のAddRoundKey演算部及び前記第２のAddRoundKey演算部にRoundKeyを供給するための鍵拡張部と、

前記復号処理の開始からのクロックサイクルをカウントし、前記復号処理を行うための制御信号を生成する制御部を有することを特徴とする請求項４又は請求項５に記載の暗号処理回路。

【請求項７】
AESの暗号処理回路であって、
第１のAddRoundKey演算部と第２のAddRoundKey演算部と第3のAddRoundKey演算部と第1のShiftRows演算部と第2のShiftRows演算部と第1のSubBytes演算部と第２のSubBytes演算部と第1のMixColumns演算部と第２のMixColumns演算部とデータ保持部を有し、
前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と前記第3のAddRoundKey演算部と前記第1のShiftRows演算部と前記第2のShiftRows演算部と前記第1のSubBytes演算部と前記第２のSubBytes演算部と前記第1のMixColumns演算部と前記第２のMixColumns演算部と前記データ保持部を用いて、複数のクロックサイクルで暗号化処理を行い、
前記暗号化処理の１つのクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と第3のAddRoundKey演算部を用い、
前記１つのクロックサイクルとは異なる、前記暗号化処理のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と前記第３のAddRoundKey演算部のうち、いずれか２つのAddRoundKey演算部を用いることを特徴とする暗号処理回路。
【請求項８】
前記暗号化処理の最初のクロックサイクルでは、平文データを、前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記第1のSubBytes演算部に入力し、前記第1のSubBytes演算部の出力を前記第1のShiftRows演算部に入力し、前記第1のShiftRows演算部の出力を前記第1のMixColumns演算部に入力し、前記第1のMixColumns演算部の出力を前記第２のAddRoundKey演算部に入力し、前記第２のAddRoundKey演算部の出力を前記第２のSubBytes演算部に入力し、前記第２のSubBytes演算部の出力を前記第２のShiftRows演算部に入力し、前記第２のShiftRows演算部の出力を前記第２のMixColumns演算部に入力し、前記第２のMixColumns演算部の出力を前記データ保持部に入力し、
前記暗号化処理の２クロックサイクル目からラウンド数Nr/2 - 1クロックサイクル目では、前記データ保持部の出力を前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記第1のSubBytes演算部に入力し、前記第1のSubBytes演算部の出力を前記第1のShiftRows演算部に入力し、前記第1のShiftRows演算部の出力を前記第1のMixColumns演算部に入力し、前記第1のMixColumns演算部の出力を前記第２のAddRoundKey演算部に入力し、前記第２のAddRoundKey演算部の出力を前記第２のSubBytes演算部に入力し、前記第２のSubBytes演算部の出力を前記第２のShiftRows演算部に入力し、前記第２のShiftRows演算部の出力を前記第２のMixColumns演算部に入力し、前記第２のMixColumns演算部の出力を前記データ保持部に入力し、
前記暗号化処理のラウンド数Nr/2クロックサイクル目では、前記データ保持部の出力を前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記第1のSubBytes演算部に入力し、前記第1のSubBytes演算部の出力を前記第1のShiftRows演算部に入力し、前記第1のShiftRows演算部の出力を前記第1のMixColumns演算部に入力し、前記第1のMixColumns演算部の出力を前記第２のAddRoundKey演算部に入力し、前記第２のAddRoundKey演算部の出力を前記第2のSubBytes演算部に入力し、前記第2のSubBytes演算部の出力を前記第2のShiftRows演算部に入力し、前記第2のShiftRows演算部の出力を前記第３のAddRoundKey演算部に入力し、前記第３のAddRoundKey演算部の出力を前記データ保持部に入力することを特徴とする請求項７に記載の暗号処理回路。
【請求項９】
CipherKeyからRoundKeyを生成し、前記第１のAddRoundKey演算部、前記第２のAddRoundKey演算部及び前記第３のAddRoundKey演算部に、前記生成したRoundKeyを供給するための鍵拡張部と、
前記暗号化処理の開始からのクロックサイクルをカウントし、前記暗号化処理を行うための制御信号を生成する制御部を有することを特徴とする請求項７又は請求項８に記載の暗号処理回路。
【請求項１０】

AESの暗号処理回路であって、
第１のAddRoundKey演算部と第２のAddRoundKey演算部と第3のAddRoundKey演算部と第1のInvShiftRows演算部と第2のInvShiftRows演算部と第1のInvSubBytes演算部と第２のInvSubBytes演算部と第1のInvMixColumns演算部と第２のInvMixColumns演算部とデータ保持部を有し、
前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と前記第3のAddRoundKey演算部と前記第1のInvShiftRows演算部と前記第2のInvShiftRows演算部と前記第1のInvSubBytes演算部と前記第２のInvSubBytes演算部と前記第1のInvMixColumns演算部と前記第２のInvMixColumns演算部と前記データ保持部を用いて、複数のクロックサイクルで復号処理を行い、
前記復号処理の１つのクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と第3のAddRoundKey演算部を用い、
前記１つのクロックサイクルとは異なる、前記復号処理のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と第3のAddRoundKey演算部のうち、いずれか２つのAddRoundKey演算部を用いることを特徴とする暗号処理回路。
【請求項１１】
前記復号処理の最初のクロックサイクルでは、暗号文データを、前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記第1のInvSubBytes演算部に入力し、前記第1のInvSubBytes演算部の出力を前記第1のInvShiftRows演算部に入力し、前記第1のInvShiftRows演算部の出力を前記第1のInvMixColumns演算部に入力し、前記第1のInvMixColumns演算部の出力を前記第２のAddRoundKey演算部に入力し、前記第２のAddRoundKey演算部の出力を前記第２のInvSubBytes演算部に入力し、前記第２のInvSubBytes演算部の出力を前記第２のInvShiftRows演算部に入力し、前記第２のInvShiftRows演算部の出力を前記第２のInvMixColumns演算部に入力し、前記第２のInvMixColumns演算部の出力を前記データ保持部に入力し、
前記復号処理の２クロックサイクル目からラウンド数Nr/2 - 1クロックサイクル目では、前記データ保持部の出力を前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記第1の前記InvSubBytes演算部に入力し、前記第1の前記InvSubBytes演算部の出力を前記第1のInvShiftRows演算部に入力し、前記第1のInvShiftRows演算部の出力を前記第1のInvMixColumns演算部に入力し、前記第1のInvMixColumns演算部の出力を前記第２のAddRoundKey演算部に入力し、前記第２のAddRoundKey演算部の出力を前記第２のInvSubBytes演算部に入力し、前記第２のInvSubBytes演算部の出力を前記第２のInvShiftRows演算部に入力し、前記第２のInvShiftRows演算部の出力を前記第２のInvMixColumns演算部に入力し、前記第２のInvMixColumns演算部の出力を前記データ保持部に入力し、
前記復号処理のラウンド数Nr/2クロックサイクル目では、前記データ保持部の出力を前記第1のAddRoundKey演算部に入力し、前記第1のAddRoundKey演算部の出力を前記第1のInvSubBytes演算部に入力し、前記第1のInvSubBytes演算部の出力を前記第1のInvShiftRows演算部に入力し、前記第1のInvShiftRows演算部の出力を前記第1のInvMixColumns演算部に入力し、前記第1のInvMixColumns演算部の出力を前記第２のAddRoundKey演算部に入力し、前記第２のAddRoundKey演算部の出力を前記第2のInvSubBytes演算部に入力し、前記第2のInvSubBytes演算部の出力を前記第2のInvShiftRows演算部に入力し、前記第2のInvShiftRows演算部の出力を前記第３のAddRoundKey演算部に入力し、前記第３のAddRoundKey演算部の出力を前記データ保持部に入力することを特徴とする請求項１０に記載の暗号処理回路。
【請求項１２】
CipherKeyからRoundKeyを生成し、前記第１のAddRoundKey演算部、前記第２のAddRoundKey演算部及び前記第３のAddRoundKey演算部に、前記生成したRoundKeyを供給するための鍵拡張部と、
前記復号処理の開始からのクロックサイクルをカウントし、前記復号処理を行うための制御信号を生成する制御部を有することを特徴とする請求項１０又は請求項１１に記載の

暗号処理回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はFIPS197(連邦情報処理規格)として規定されているAES（Advanced Encryption Standard）処理を実行するための暗号処理回路に関する。
【背景技術】
【０００２】
近年、光ファイバ網の整備が進み、インターネット上での高速な通信を誰もが容易に利用できるようになった。それにより、高画質な映像配信などといった大容量のデータ通信が手軽に行えるようになった。しかし、ネットワークには盗聴、改竄、なりすましといった脅威が存在する。そこで、それらの脅威からネットワーク通信を保護するため、暗号化へのニーズが高まっている。
【０００３】
しかし、安全な通信を行うためには暗号化は必須であるものの、暗号化を行うゆえに通信速度が低下するようなことは好ましくない。映像配信のように大容量のデータを扱う分野においてその傾向は顕著である。そこで、大容量のデータを、セキュアかつ高速に通信するため、高速な暗号化処理が求められている。
【０００４】
大容量の暗号化通信では、一般的に共通鍵暗号が用いられている。
【０００５】
その共通鍵暗号の中で、現在もっとも広く用いられているのがFIPS（Federal Information Processing Standards）197にて規定されるAESである。
【０００６】
高速な暗号化通信に対応するためにはAESを専用のハードウェアアクセラレータで高速化する必要がある。
【０００７】
ここで、AESの暗号化処理、復号処理のアルゴリズムを図６０に示す。ただし、図６０におけるAddRoundKey、SubBytes、ShiftRows、MixColumns、InvSubBytes、InvShiftRows、InvMixColumnsは、FIPS197にてサブブロック演算として規定される同名の処理である。また、NRは鍵長に応じて決定されるラウンド数という定数であり、AES-128では10、AES-192では12、AES-256では14である。
【０００８】
同図に示すようにAESのアルゴリズムはAddRoundKey演算の後、規格にて定義されるラウンド処理をNR回繰り返す手順となっている。ラウンド処理は暗号化時にはSubBytes、ShiftRows、MixColumns、AddRoundKeyの4つの処理、復号時にはInvShiftRows、InvSubBytes,AddRoundKey、InvMixColumnsの4つの処理である。ただし、例外として、NR回目の実行においては、暗号化時はSubBytes、ShiftRows、AddRoundKeyの3つの処理、復号時はInvShiftRows、InvSubBytes,AddRoundKeyの3つの処理となる。また、AddRoundKeyの演算には共通鍵より生成する実行鍵wkeyi（FIPS197記載のRound Key、iはラウンド数を示す）が必要でありその値はラウンドごとにすべて異なる。ただし、wkey0は共通鍵と等しい。
【０００９】
このAESをハードウェアとして実装するには、AES処理回路に供給されるクロックの1クロックサイクル内に収まるように処理を分割しなければならない。従来の一般的な実装方法では、先述したラウンド処理を処理の区切りと捉えて実装していた。例えば、1クロックサイクル内にラウンド処理を1回実行する、1クロックサイクル内にラウンド処理を2回実行する、2クロックサイクル内にラウンド処理を1回実行するといった実装法が一般的である。従来手法の場合、AES-128の暗号化処理、復号処理には、それぞれ11クロックサイクル、6クロックサイクル、22クロックサイクルを要する。
【特許文献１】http://www.ocean-logic.com/pub/OL_AES.pdf　OceanLogic社製 AES Core

Family V1.5
【発明の開示】
【発明が解決しようとする課題】
【００１０】
AESをハードウェアで実現することで、ある一定レベルの高速処理を得ることができるが、AESの処理速度はさらなる高速化が求められている。
【００１１】
以上の点を鑑み、本発明は暗号化処理、復号処理に要するサイクル数を削減し、より高速にAES処理を実行する暗号処理回路を提供することを目的とする。
【課題を解決するための手段】
【００１２】
上記課題を解決するため、本発明は、AESの暗号処理回路であって、
第１のAddRoundKey演算部と第２のAddRoundKey演算部とShiftRows演算部とSubBytes演算部とMixColumns演算部とデータ保持部を有し、
前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部と前記ShiftRows演算部と前記SubBytes演算部と前記MixColumns演算部と前記データ保持部を用いて、複数のクロックサイクルで暗号化処理を行い、
前記暗号化処理の最後のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部を用い、かつ、前記MixColumns演算部を用いず、
前記最後のクロックサイクルを除く、前記暗号化処理のクロックサイクルでは、前記第１のAddRoundKey演算部と前記第２のAddRoundKey演算部のうち、いずれか１つのAddRoundKey演算部を用いることを特徴とする。
【発明の効果】
【００１３】
本発明によれば、各クロックサイクル内で実行する処理の処理時間ができるだけ均等になるよう、AESの暗号化処理、復号処理の処理の区切りを変更した。それにより、各ハードウェアによってAESの暗号化処理、復号処理を行う際に要するサイクル数を従来より削減することができる。
【００１４】
本発明を実施した場合の各クロックサイクル内で実行する処理の処理時間の最大値は、従来技術のそれと等しいため、サイクル数の削減はすなわち処理速度の向上となる。
【００１５】
本発明は暗号化処理、復号処理（Equivalent Inverse Cipherを含む）の両方に対して適用可能である。本発明は、1Round/Cycle、2Round/cycle、0.5Round/Cycleといった実装法を問わず適用可能である。さらに、本発明はECBモード、CBCモード等といった暗号モードを問わずに適用可能である。また、本発明はすべての鍵長に対して適用可能である。
【００１６】
本発明の効果として、1Round/Cycleの実装法では、AES-128において11サイクルから10サイクルに、AES-192において13サイクルから12サイクルに、AES-256において15サイクルから14サイクルにそれぞれ削減することができる。また、2Round/Cycleの実装法では、AES-128において6サイクルから5サイクルに、AES-192において7サイクルから6サイクルに、AES-256において8サイクルから7サイクルにそれぞれ削減することができる。
【発明を実施するための最良の形態】
【００１７】
以下、添付図面に従って本発明に係る実施形態を詳細に説明する。なお、本実施形態では、FIPS197に定義されるAES-128（以下、単にＡＥＳと略記する）を例にとって説明する。
【００１８】
＜第１の実施形態＞
図１は第１の実施形態における各クロックサイクル内で実行される暗号化処理の処理内

容を従来例と比較して示したものである。

【００１９】

同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。また、実行鍵wkeyi（iはラウンド数を示す）はFIPS197記載のRound Keyのことである。

【００２０】

本実施形態は、０サイクル目から８サイクル目ではAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算を実行する。そして、９サイクル目では、第１のAddRoundKey演算、ShiftRows演算、SubBytes演算、第２のAddRoundKey演算を実行する。実行鍵は0サイクル目ではwkey0、1サイクル目ではwkey1、…、８サイクル目ではwkey8が用いられ、9サイクル目では２つの実行鍵wkey9、wkey10が必要となる。

【００２１】

本実施形態は従来と比較して、トータルで実行している処理は同じであるが、本実施形態ではAESの暗号化処理を1つ少ないクロックサイクル数で実行することができる。

【００２２】

次に、本実施形態において各クロックサイクル内で実行される暗号化処理に必要な処理時間について述べる。図２は、従来技術と第１の実施形態における各クロックサイクル内で実行される暗号化処理に必要な処理時間を比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図２に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。

【００２３】

本実施形態では、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行う０～８サイクル目の処理に必要な処理時間は、AddRoundKey演算、SubBytes演算、ShiftRows演算、AddRoundKey演算を行う9サイクル目の処理に必要な処理時間よりも長い。したがって、本実施形態において1サイクル内で実行される処理に必要な処理時間の最大値を従来技術のものと比較すると、両者は等しい。従来技術において1サイクル内で実行される処理に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態もまた実施可能である。

【００２４】

本発明はAESの復号処理についても同様に適用可能である。

【００２５】

図３は実施形態において各クロックサイクル内で実行される復号処理の処理内容を従来例と比較して示したものである。

【００２６】

同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。

【００２７】

本実施形態は、0サイクル目では第１のAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、第２のAddRoundKey演算を行う。そして、１サイクル～９サイクル目ではInvMixColumns演算、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算を実行する。実行鍵は0サイクル目では2つの実行鍵wkey9とwkey10、1サイクル目ではwkey8、２サイクル目ではwkey7、…、9サイクル目ではwkey0が用いられる。

【００２８】

本実施形態と従来技術はトータルで実行している処理は同じであるが、本実施形態ではAESの復号処理を1つ少ないクロックサイクル数で実行することができる。

【００２９】

次に、本実施形態において各クロックサイクル内で実行される復号処理に必要な処理時間について述べる。図４は、第１の実施形態において各クロックサイクル内で実行される

復号処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図４に示すように、各サブブロック演算の処理時間は、InvSubBytes演算がもっとも長く、次いでInvMixColumns演算、AddRoundKey演算、InvShiftRows演算である。

【００３０】

本実施形態では、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行う１～９サイクル目の処理に必要な処理時間は、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、AddRoundKey演算を行う０サイクル目の処理に必要な処理時間よりも長い。本実施形態において1サイクル内で実行される処理に必要な処理時間の最大値を従来技術のものと比較すると、両者は等しい。従来技術において1サイクル内で実行される処理に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態もまた実施可能である。

【００３１】

ここまでで説明してきた本発明の特徴についてまとめる。

【００３２】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、10サイクル目と0サイクル目に実行される処理に必要な処理時間を合わせても、１～９サイクル目に実行される処理に必要な処理時間に及ばないというように、1サイクル内で実行される処理に必要な処理時間にばらつきがあった。

【００３３】

一方、本発明では1サイクル内で実行される処理に必要な処理時間を均等にするよう暗号化処理、復号処理の処理の区切りを変更した。本発明は1サイクル内に実行される処理に必要な処理時間を増やすことなく、AESの暗号化処理、復号処理に要するクロックサイクル数を1サイクル削減しており、これにより約10%程度の処理速度の向上が得られる。

【００３４】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。

【００３５】

図５は、本実施形態のAES処理回路のブロック図を示したものである。

【００３６】

図５において、101はAESの処理を実行するAES処理回路、102は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。103は鍵拡張部102より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。104はAES処理回路101の外部からの制御信号を受け、鍵拡張部102および暗号化・復号処理部103の動作を制御するための信号を生成し、かつAES処理回路101の外部に対して動作完了を通知するための信号を生成する制御部である。

【００３７】

同図において、150は暗号化処理の対象となる平文データもしくは復号処理の対象となる暗号文データであるところの入力信号である。151は暗号化・復号処理部103において入力信号150を暗号化、または復号処理した結果であるところの出力信号である。152は暗号化・復号処理で用いられる共通鍵、153は暗号化処理、復号処理のどちらを行うかを選択するための暗号化・復号選択信号である。155は鍵拡張部102において共通鍵152から実行鍵を生成する鍵拡張を開始させるための鍵準備開始信号、157は暗号化処理または復号処理が１サイクル後に実行可能となることを示す暗号化・復号処理許可信号である。158は入力信号150に対して暗号化処理または復号処理を開始させるための暗号化・復号処理開始信号、159は暗号化・復号処理部103において暗号化または復号処理を行った結果が出力信号151に保持されていることを示す有効出力期間信号である。160は暗号化・復号処理部

103に対して出力信号151を一定値に保持せしめるための出力保持制御信号である。161は鍵準備や暗号化・復号処理の際に、鍵準備開始信号155または暗号化・復号処理開始信号158の立ち上がりからのサイクル数を示すカウンタ信号である。162は実行鍵のうちの一つであるところの実行鍵Ａである。163は鍵拡張部102で生成された暗号化処理の最後のサイクルで使用される実行鍵、もしくは復号時の最初のサイクルで使用される実行鍵であるところの実行鍵Ｂである。170は暗号化・復号処理部103においてサブブロック演算の接続を切り替えるための選択信号、171は暗号化・復号処理部103において被処理データを切り替えるための選択信号である。

【００３８】

上記構成において、外部からの入力信号150は暗号化・復号処理部103に入力され、出力信号151は暗号化・復号処理部103より外部に対して出力される。共通鍵152は外部より鍵拡張部102に対して入力され、暗号化・復号選択信号153は外部より鍵拡張部102、暗号化・復号処理部103および制御部104に対して入力される。鍵準備開始信号155は外部より鍵拡張部102および制御部104に対して入力される。暗号化・復号処理許可信号157は制御部104より外部に対して出力され、暗号化・復号処理開始信号158は外部より鍵拡張部102および制御部104に対して入力される。有効出力期間信号159は制御部104より外部に対して出力され、出力保持制御信号160は制御部104より暗号化・復号処理部103に対して入力される。カウンタ信号161は制御部104から鍵拡張部102に対して出力され、実行鍵Ａ（参照番号162、以下、同様）は鍵拡張部102から暗号化・復号処理部103に対して出力される。実行鍵Ｂ（163）は鍵拡張部102から暗号化・復号処理部103に対して出力される。選択信号170は制御部104から暗号化・復号処理部103に対して出力され、選択信号171は制御部104から暗号化・復号処理部103に対して出力される。

【００３９】

次に、暗号化・復号処理部103について説明する。図６は暗号化・復号処理部103のブロック図を示したものである。同図において、105は、選択信号170による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて1サイクル分の暗号化処理を行うラウンド処理部である。106は選択信号170による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて復号処理を行うラウンド処理部である。

【００４０】

107は暗号化・復号選択信号153に応じて、ラウンド処理部105の出力、もしくはラウンド処理部106の出力のいずれかを選択するためのセレクタである。108は出力保持制御信号160に応じてセレクタ107により選択された信号を保持するデータ保持部である。109は選択信号171に応じて、入力信号150、もしくはデータ保持部108の出力信号のいずれかを選択するためのセレクタである。

【００４１】

同図において、165はラウンド処理部105およびラウンド処理部106への入力信号、166は入力信号165に対してラウンド処理部105で処理を施した結果であるところの出力信号である。167は入力信号165に対してラウンド処理部106で処理を施した結果であるところの出力信号、168はセレクタ107の出力信号である。

【００４２】

上記構成において、セレクタ109には入力信号150、データ保持部の出力データおよび選択信号171が入力される。ラウンド処理部105にはセレクタ109の出力、実行鍵Ａ（162）、実行鍵Ｂ（163）、選択信号170が入力される。ラウンド処理部106にはセレクタ109の出力、実行鍵Ａ（162）、実行鍵Ｂ（163）、選択信号170が入力される。セレクタ107にはラウンド処理部105の出力信号、ラウンド処理部106の出力信号および暗号化・復号処理選択信号153が入力される。データ保持部108にはセレクタ107の出力およびデータ保持制御信号160が入力される。そして、データ保持部108は暗号化・復号処理部103の出力信号151を出力する。

【００４３】

また、上記構成において、セレクタ109は、選択信号171がNegateされている時は入力信

号150、Assertされている時はデータ保持部108の出力信号151を選択し出力する。セレクタ109により選択された結果であるところの入力信号165は、ラウンド処理部105およびラウンド処理部106に入力され、それぞれ暗号化処理、復号処理を施される。セレクタ107は暗号化・復号選択信号153がNegateされている時はラウンド処理部105の出力結果であるところの出力信号166、Assertされている時はラウンド処理部106の出力結果であるところの出力信号167を選択し、出力する。セレクタ107の出力信号168は、データ保持部108へ入力され、一時保持される。データ保持部108の出力信号151は暗号化・復号処理部103の出力信号である。同時にセレクタ109の入力へも接続されており、セレクタ信号171がAssertされている間、ラウンド処理部105における暗号化処理、またはラウンド処理部106による復号処理が繰り返し実行される。

【００４４】

暗号化・復号処理が終了し、かつ次なる暗号化・復号処理が開始されていない場合、制御部104により出力保持制御信号160がAssertされる。その間、データ保持部108は出力信号168によらず出力信号151を一定値に保持し続ける。

【００４５】

次に、ラウンド処理部105について説明する。図７はラウンド処理部105のブロック図について示したものである。同図において、110は入力信号165および実行鍵Ａ（162）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部（第１のAddRoundKey演算部に相当）である。111はAddRoundKey演算部110の出力を入力としSubBytes演算を行うところのSubBytes演算部である。112はSubBytes演算部111の出力を入力としShiftRows演算を行うところのShiftRows演算部である。113はShiftRows演算部112の出力を入力とし、MixColumns演算を行うところのMixColumns演算部である。114はShiftRows演算部112の出力および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部（第２のAddRoundKey演算部に相当）である。115は選択信号170に応じてMixColumns演算部113の出力、もしくはAddRoundKey演算部114の出力のいずれか一方を選択し、出力するセレクタである。セレクタ115の出力信号はラウンド処理部105の出力となる。

【００４６】

上記構成において、セレクタ115は選択信号170がNegateされている時はMixColumns演算部の出力、Assertされている時はAddRoundKey演算部の出力を選択し、出力する。

【００４７】

次に、ラウンド処理部106について、図８のブロック図を参照して説明する。

【００４８】

同図において、116は入力信号165を入力としInvMixColumns演算を行うところのInvMixColumns演算部である。117は入力信号165および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。118は選択信号170に応じて、InvMixColumns演算部116の出力かAddRoundKey演算部117の出力のいずれか一方を選択し、出力するセレクタである。119はセレクタ118の出力を入力としInvShiftRows演算を行うところのInvShiftRows演算部である。120はInvShiftRows演算部119の出力を入力としInvSubBytes演算を行うところのInvSubBytes演算部である。121はInvSubBytes演算部120の出力を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。AddRoundKey演算部121の出力はラウンド処理部106の出力となる。

【００４９】

上記構成において、セレクタ118は選択信号170がNegateされている時InvMixColumns演算部116の出力、Assertされている時はAddRoundKey演算部117の出力を選択し、出力する。

【００５０】

次に、上記構成における暗号化処理時の動作について説明する。図９は本実施形態の暗号化処理時のタイミングチャートを示したものである。図９において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、・・・、T33とタイミング名が割り当てられている。

【００５１】
同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図５～図８で使用されている信号線のナンバと一対一で対応している。
【００５２】
図９のタイミングチャートに示される暗号化処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の暗号化処理期間（T17～T27）である。そして、４つ目は、2ブロック目の暗号化処理期間（T27以降）である。
【００５３】
パラメータ設定では、共通鍵152、暗号化・復号選択信号153の他、必要に応じて鍵長や暗号モードなど暗号化・復号処理の各種パラメータが設定される。暗号化・復号選択信号153および共通鍵152の値は、新たにパラメータ設定が行われるまで外部より値が常に保持されている必要がある。パラメータ設定期間はリセット直後からの任意長の期間であり、AES処理回路101の外部より鍵準備開始信号155がAssertされると（T06）、パラメータ設定期間が終了する。
【００５４】
パラメータ設定期間が終了すると同時に、次の鍵準備期間が開始される。鍵準備期間は、暗号処理の９サイクル目（T26）において、鍵拡張部102が2つの実行鍵（wkey9、wkey10）を暗号化・復号処理部103に対して同時に供給するために、事前に最後の実行鍵（wkey10）を生成するための期間である。鍵準備期間は鍵準備開始信号155がAssertされてから（T06）、最後の実行鍵（wkey10）が生成される11サイクル後（T17）までの期間である。
【００５５】
次に、鍵準備期間における各回路の動作について述べる。まず、鍵準備開始信号155がAssertされると、制御部104はカウンタ信号161を0から順次カウントアップする。鍵拡張部102はカウンタ信号161に合わせてwkey0（共通鍵152）を各クロックサイクルごとに拡張していき、10個の実行鍵wkey1、wkey2、…、wkey10を生成していく。生成された実行鍵は実行鍵Ａ（162）より順次出力されるようになっている。
【００５６】
タイミングT16でカウンタ信号161が”10”になると、鍵拡張部102は、生成した実行鍵（wkey10）をレジスタに保持し、実行鍵Ｂ（163）より出力する。以後、wkey10は、再び鍵準備が実行されるまで保持され続ける。
【００５７】
鍵準備期間が終了すると（T17）、鍵拡張部102は、暗号化・復号処理で最初に用いられる実行鍵（暗号化時はwkey0、復号時はwkey9）を実行鍵Ａ（162）より出力する。実行鍵Ａ（162）の値は、暗号化・復号処理開始信号158がAssertされるまで保持される。そして、制御部104はカウンタ信号161のカウントアップを停止し、カウンタをゼロクリアする。
【００５８】
また、鍵準備期間の終了に合わせ、制御部104はT16において、T17で鍵準備が終了し、暗号化処理が可能となることを見越し、暗号化・復号処理許可信号157をAssertする。
【００５９】
AES処理回路101の外部にある入力信号供給部は、T17で暗号化・復号処理許可信号157のAssertを検知すると、入力信号150として平文データP0をAES処理回路101に供給する。そして、入力信号150に対する暗号化処理を開始せしめるため、暗号化・復号処理開始信号158をAssertする(T17)。なお、このタイミングチャートでは最短のサイクルで暗号化・復号処理開始信号158がAssertされているが、そのタイミングはAES処理回路101の外部で自由に決められる。
【００６０】
暗号化処理期間は、入力信号150に対して暗号化処理を行う期間である。暗号化処理期間は、暗号化・復号処理開始信号158がAssert（T17）されてから、その10サイクル後（T2

7）までの期間である。

【００６１】

制御部104は暗号化・復号処理開始信号158のAssertを検知すると、次サイクル（T18）で暗号化・復号処理許可信号157、有効出力期間信号159、出力保持制御信号160をNegateする。同時に、カウンタ信号161のカウントアップを開始する。

【００６２】

鍵拡張部102は、カウンタ信号161にしたがって実行鍵wkey0から順次鍵拡張を行い、T18ではwkey1、T19ではwkey2、…、T26ではwkey9を実行鍵Ａ（162）として暗号化・復号処理部103に出力する。

【００６３】

ラウンド処理部105はT17～T18では選択信号171がNegateされているため、入力信号150に対して、実行鍵Ａとして出力されているwkey0を用いて各サブブロック演算を行う。そして、T18～T27では選択信号171がAssertされているため、データ保持部108の出力に対して、T18～T19ではwkey1、T19～T20ではwkey2、…、T25～T26ではwkey8を用いてサブブロック演算を行う。

【００６４】

暗号化処理の最終サイクルになると（T26）、制御部104は選択信号170をAssertする。それを受け、ラウンド処理部105のセレクタ115は、実行鍵Ｂ（163）を用いてAddRoundKey演算を行うAddRoundKey114の出力を選択し、最終サイクルのサブブロック演算を行う。T26において、ラウンド処理部105の出力信号166は入力信号である平文データP0を暗号化した結果である暗号文データC0を出力しており、その値は1サイクル後（T27）にデータ保持部108よりAES処理回路101の出力として、外部に出力される。同時に、制御部104は暗号化処理が終了し、出力信号151が有効であることをAES処理回路101の外部に対して通知するため、有効出力期間信号159をAssertする(T27)。有効出力期間信号159がAssertされている間、AES処理回路101は出力信号151が有効であることを保証する。

【００６５】

一方、出力保持制御信号160は、T27において有効出力期間信号159がAssertされているものの、同じくT27において暗号化・復号処理開始信号158もまたAssertされているため、Negateされたままである。もしT27において暗号化・復号処理開始信号158がAssertされなかった場合、T27において出力保持制御信号160がAssertされ、データ保持部108の値は暗号文データC0に保持される。

【００６６】

また、鍵拡張部102は暗号化処理が終了するT27において、実行鍵Ａ（162）よりwkey0を出力する。そして、実行鍵A162の値は、次なる暗号化・復号処理開始信号156がAssertされるまで保持される。

【００６７】

さらに、制御部104は暗号化処理の完了（T27）を見越し、完了の1サイクル前（T26）に暗号化・復号処理許可信号157をAssertする。AES処理回路101の外部は、暗号化・復号処理許可信号157がAssertされていると、入力信号150の値を次なる平文データP1とし、2ブロック目の暗号化処理を開始することが可能となる。図９のタイミングチャートでは、AES処理回路101の外部は、最短のサイクルで次なる暗号化・復号処理開始信号をAssertしている(T27)。図９のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には暗号化処理の間隔は任意の長さとすればよい。2ブロック目以降の暗号化処理では、1ブロック目と同様の動作が繰り返し行われる。

【００６８】

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【００６９】

続いて、本実施形態の復号処理の動作について説明する。図１０は本実施形態の復号処理時のタイミングチャートについて示したものである。同図において横軸は時間を示しており、クロックの立ち上がりごとにT01、T02、・・・、T33のタイミング名が割り当てられている。また、同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図５～図８で使用されている信号線のナンバと一対一で対応している。

【００７０】

復号処理時の動作もパラメータ設定期間（T01～T06）、鍵準備期間（T06～T17）、1ブロック目の復号処理期間（T17～T27）、2ブロック目の復号処理期間（T27以降）の4つに大別される。

【００７１】

パラメータ設定期間はT01～T06までの期間であり、その役割、開始条件、終了条件は本実施形態の暗号化処理時と同様である。ただし、復号処理時は暗号化・復号処理選択信号153はAssertされる。

【００７２】

鍵準備期間はT06～T17までであり、開始条件および終了条件は本実施形態の暗号化処理時と同様である。各回路の動作も本実施形態の暗号化処理時とほぼ同様である。ただし、暗号化処理と復号処理では最初のサイクルで用いられる実行鍵が異なるため、鍵拡張部102は鍵準備期間の終了時（T17）にwkey10より逆順に鍵拡張を行い、wkey9を生成し、実行鍵Ａ（162）より出力する。実行鍵Ａ（162）の値は、暗号化・復号処理開始信号158がAssertされるまで保持される。そして、制御部104はカウンタ信号161のカウントアップを停止し、カウンタをゼロクリアする。

【００７３】

また、鍵準備期間の終了に合わせ、制御部104はT16において、T17で鍵準備が終了し、復号処理が可能となることを見越し、暗号化・復号処理許可信号157をAssertする。

【００７４】

AES処理回路101の外部にある入力信号供給部は、T17で暗号化・復号処理許可信号157のAssertを検知すると、入力信号150として暗号文データC0をAES処理回路101に供給する。そして、入力信号150に対する復号処理を開始せしめるため、暗号化・復号処理開始信号158をAssertする(T17)。なお、このタイミングチャートでは最短のサイクルで暗号化・復号処理開始信号158がAssertされているが、そのタイミングはAES処理回路101の外部で自由に決められる。

【００７５】

復号処理期間は、入力信号150に対して復号処理を行う期間である。復号処理期間は、暗号化・復号処理開始信号158がAssert（T17）されてから、その10サイクル後（T27）までの期間である。

【００７６】

制御部104は暗号化・復号処理開始信号158のAssertを検知すると、次サイクル（T18）で暗号化・復号処理許可信号157、有効出力期間信号159、出力保持制御信号160をNegateする。同時に、カウンタ信号161のカウントアップを開始する。

【００７７】

鍵拡張部102は、カウンタ信号161にしたがって実行鍵wkey9から逆順に鍵拡張を行い、T18ではwkey9、T19ではwkey8、…、T26ではwkey0を実行鍵Ａ（162）として暗号化・復号処理部103に出力する。

【００７８】

ラウンド処理部106はT17～T18では選択信号171がNegateされているため、入力信号150に対して実行鍵Ａとして出力されているwkey9を用いて各サブブロック演算を行う。制御部104は、復号時には最初のサイクルにおいて選択信号170をAssertする。それを受け、ラウンド処理部106のセレクタ118は、実行鍵Ｂ（163）を用いてAddRoundKey演算を行うAddRoundKey117の出力を選択し、最初のサイクルのサブブロック演算を行う。

【００７９】

そして、T18～T27では選択信号171がAssertされているため、データ保持部108の出力に対して、T18～T19ではwkey8、T19～T20ではwkey7、…、T26～T27ではwkey0を用いてサブブロック演算を行う。

【００８０】

T26において、ラウンド処理部106の出力信号167は入力信号である暗号文データC0を復号した結果である平文データP0を出力しており、その値は1サイクル後（T27）にデータ保持部108よりAES処理回路101の出力として、外部に出力される。同時に、制御部104は復号処理が終了し、出力信号151が有効であることをAES処理回路101の外部に対して通知するため、有効出力期間信号159をAssertする(T27)。有効出力期間信号159がAssertされている間、AES処理回路101は出力信号151が有効であることを保証する。

【００８１】

一方、出力保持制御信号160は、T27において有効出力期間信号159がAssertされているものの、同じくT27において暗号化・復号処理開始信号158もまたAssertされているため、Negateされたままである。もしT27において暗号化・復号処理開始信号158がAssertされなかった場合、T27において出力保持制御信号160がAssertされ、データ保持部108の値は平文データP0に保持される。

【００８２】

また、鍵拡張部102は復号処理が終了するT27において、wkey10よりwkey9を逆算で求め、実行鍵Ａ（162）より出力する。そして、実行鍵A162の値は、次なる暗号化・復号処理開始信号156がAssertされるまで保持される。

【００８３】

さらに、制御部104は復号処理の完了（T27）を見越し、完了の1サイクル前（T26）に暗号化・復号処理許可信号157をAssertする。AES処理回路101の外部は、暗号化・復号処理許可信号157がAssertされていると、入力信号150の値を次なる暗号文データC1とし、2ブロック目の復号処理を開始することが可能となる。図１０のタイミングチャートでは、AES処理回路101の外部は、最短のサイクルで次なる暗号化・復号処理開始信号158をAssertしている(T27)。2ブロック目の復号処理の動作は1ブロック目と同様に行われる。以降、任意の回数復号処理の動作が繰り返される。

【００８４】

すべての復号処理が終了し、次なるジョブを開始する際には、再びパラメータ設定から始まる。

【００８５】

第１の実施形態は以上のようにして実施可能である。第１実施形態は、１サイクル内で実行しなければならない処理の処理時間の最大値を増やすことなく、AESの暗号化処理に要するクロックサイクル数を1サイクル削減している。これにより約10%程度の処理速度の向上が得られる。

【００８６】

＜第２の実施形態＞

図１１は第２の実施形態において各クロックサイクル内で実行される暗号化処理、復号処理の処理内容を示した図である。

【００８７】

同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。

【００８８】

本実施形態の暗号化処理は、0サイクル目では、第１のAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算、第２のAddRoundKey演算を実行する。そして、１サイクル目から８サイクル目ではAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算を実行する。そして、９サイクル目では、AddRoundKey演算、ShiftRows演算、SubBytes演算を実行する。実行鍵は0サイクル目ではwkey0とwkey1、1サイクル目ではwkey2、…、９サイクル目ではwkey10が用いられる。

【００８９】
本第２の実施形態は従来技術とトータルで実行している処理は同じであるが、本実施形態ではAESの暗号化処理を1つ少ないクロックサイクル数で実行することができる。
【００９０】
次に、本第２の実施形態において各クロックサイクル内で実行される処理に必要な処理時間について述べる。図１２は、本第２の実施形態において各クロックサイクル内で実行される処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第２の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図１２に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。
【００９１】
本実施形態では、第１のAddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算、第２のAddRoundKey演算を行う０サイクル目の処理に必要な処理時間は、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行う１～８サイクル目の処理に必要な処理時間や、AddRoundKey演算、SubBytes演算、ShiftRows演算を行う９サイクル目の処理に必要な処理時間よりも長い。したがって、本実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。
【００９２】
本発明はAESの復号処理についても同様に適用可能である。
【００９３】
図１１に示すように、本実施形態の復号処理は、0サイクル目ではAddRoundKey演算、InvShiftRows演算、InvSubBytes演算を実行する。そして、１サイクル目から８サイクル目ではAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、InvMixColumns演算を実行する。そして、９サイクル目では、第１のAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、InvMixColumns演算、第２のAddRoundKey演算を実行する。実行鍵は0サイクル目ではwkey10、１サイクル目ではwkey9、…、８サイクル目ではwkey2が用いられ、9サイクル目では２つの実行鍵wkey1、wkey0が必要となる。
【００９４】
本第２の実施形態は従来技術とトータルで実行している処理は同じであるが、本第２の実施形態ではAESの復号処理を1つ少ないクロックサイクル数で実行することができる。
【００９５】
次に、本第２の実施形態において各クロックサイクル内で実行される処理に必要な処理時間について述べる。図１３は、第２の実施形態において各クロックサイクル内で実行される処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図１３に示すように、各サブブロック演算の処理時間は、InvSubBytes演算がもっとも長く、次いでInvMixColumns演算、AddRoundKey演算、InvShiftRows演算である。
【００９６】
本第２の実施形態では、第１のAddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算、第２のAddRoundKey演算を行う９サイクル目の処理に必要な処理時間は、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行う１～８サイクル目の処理に必要な処理時間や、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算を行う０サイクル目の処理に必要な処理時間よりも長い。したがって、本

第２の実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本第２の実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。

【００９７】

ここまでで説明してきた本第２の実施形態の特徴についてまとめる。

【００９８】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、10サイクル目と0サイクル目に実行される処理に必要な処理時間を合わせても、１～９サイクル目に実行される処理に必要な処理時間に及ばないというように、1サイクル内で実行される処理に必要な処理時間にばらつきがあった。

【００９９】

一方、本発明では1サイクル内で実行される処理に必要な処理時間を均等にするよう暗号化処理、復号処理の処理の区切りを変更した。

【０１００】

本実施形態は1サイクル内で実行される処理に必要な処理時間の最大値をわずかに増やすため、従来技術が実施可能な条件下で必ずしも本実施形態が実施可能であるとは限らない。しかし、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理および復号処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０１０１】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。

【０１０２】

図１４は、本実施形態のAES処理回路のブロック図を示したものである。

【０１０３】

図１４において、131はAESの処理を実行するAES処理回路である。132は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。133は鍵拡張部132より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。134はAES処理回路131の外部からの制御信号を受け、鍵拡張部132および暗号化・復号処理部133の動作を制御するための信号を生成し、かつAES処理回路131の外部に対して動作完了を通知するための信号を生成する制御部である。

【０１０４】

同図において、175は制御部134より暗号化・復号処理部133に対して出力され、暗号化・復号処理部133においてサブブロック演算の接続を切り替えるための選択信号である。なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略する。

【０１０５】

次に、暗号化・復号処理部133について説明する。図１５は暗号化・復号処理部133のブロック図について説明したものである。同図において、135は、選択信号170および選択信号175による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて1サイクル分の暗号化処理を行うラウンド処理部である。136は選択信号170および選択信号175による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて復号処理を行うラウ

ンド処理部である。

【０１０６】

上記構成において、暗号化・復号処理部133のセレクタ109は、選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。

【０１０７】

なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略した。

【０１０８】

次に、ラウンド処理部135について説明する。図１６はラウンド処理部135のブロック図を示したものである。同図において、114は入力信号165および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。137は選択信号175に応じて入力信号165とAddRoundKey演算部114の出力のいずれか一方を選択し出力するセレクタである。111はセレクタ137の出力を入力としSubBytes演算を行うところのSubBytes演算部である。112はSubBytes演算部111の出力を入力としShiftRows演算を行うところのShiftRows演算部である。113はShiftRows演算部112の出力を入力とし、MixColumns演算を行うところのMixColumns演算部である。115は選択信号170に応じてMixColumns演算部113の出力とShiftRows演算部112の出力のいずれか一方を選択し出力するセレクタである。110はセレクタ115の出力および実行鍵Ａ（162）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。AddRoundKey演算部110の出力信号はラウンド処理部135の出力となる。

【０１０９】

上記構成において、セレクタ115は選択信号170がNegateされている時はMixColumns演算部113の出力、Assertされている時はShiftRows演算部112の出力を選択し、出力する。セレクタ137は選択信号175がNegateされている時は入力信号165、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。

【０１１０】

次に、ラウンド処理部136について説明する。図１７はラウンド処理部136のブロック図について示したものである。同図において、121は入力信号165および実行鍵Ａ（162）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。116はAddRoundKey演算部121の出力を入力としInvMixColumns演算を行うところのInvMixColumns演算部である。118は選択信号170に応じて、InvMixColumns演算部116の出力かAddRoundKey演算部121の出力のいずれか一方を選択し、出力するセレクタである。119はセレクタ118の出力を入力としInvShiftRows演算を行うところのInvShiftRows演算部である。120はInvShiftRows演算部119の出力を入力としInvSubBytes演算を行うところのInvSubBytes演算部である。117はInvSubBytes演算部120の出力および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。138は選択信号175に応じて、InvSubBytes演算部120の出力かAddRoundKey演算部117の出力のいずれか一方を選択し、出力するセレクタである。セレクタ138の出力はラウンド処理部136の出力となる。

【０１１１】

上記構成において、セレクタ118は選択信号170がNegateされている時InvMixColumns演算部116の出力、Assertされている時はAddRoundKey演算部121の出力を選択し出力する。セレクタ138は選択信号175がNegateされている時はInvSubBytes演算部120の出力、Assertされている時はAddRoundKey演算部117の出力を選択し出力する。

【０１１２】

次に、上記構成における暗号化処理時の動作について説明する。図１８は本第２の実施形態の暗号化処理時のタイミングチャートを示したものである。図１８において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、・・・、T33とタイミング名が割り当てられている。同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図１４～図１７で使用されている信号線のナンバと一対一で対応している。

【０１１３】

図１８のタイミングチャートに示される暗号化処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の暗号化処理期間（T17～T27）、そして。４つ目は、2ブロック目の暗号化処理期間（T27以降）である。

【０１１４】

パラメータ設定期間の役割、開始条件、終了条件は第１の実施形態と同様である。また、鍵準備期間はT06～T17までであり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。ただし、タイミングT16における鍵拡張部132の動作、およびT17における鍵拡張部132と制御部134の動作には、第１の実施形態とは異なる点があるので、それについて述べる。

【０１１５】

タイミングT16において、鍵拡張部132は実行鍵Ｂ（163）よりwkey0を出力する。ただし、wkey10は鍵拡張部132の内部に設けられたレジスタに保持されている。

【０１１６】

タイミングT17において、鍵拡張部132は実行鍵Ａ（162）よりwkey1を出力する。また、制御部134は選択信号175をAssertする。

【０１１７】

1ブロック目の暗号化処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０１１８】

制御部134は選択信号175を暗号化処理の終了時にAssertし、暗号化処理の１サイクル目(T18,T28)にNegateする。そして、選択信号170を暗号化処理の最終サイクル（T16）でAssertし、暗号化処理の終了時（T17）にNegateする。さらに、選択信号171を暗号化処理の１サイクル目にAssertし、暗号化処理の終了時にNegateする。

【０１１９】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ115は選択信号170がNegateされている時はMixColumns演算部113の出力、Assertされている時はShiftRows演算部112の出力を選択し出力する。また、セレクタ137は選択信号175がNegateされている時は入力信号165、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。

【０１２０】

したがって、ラウンド処理部135は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行う。1サイクル目からは1サイクル時間前の結果に対して、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行った結果を出力する。そして、9サイクル目（T26～T27）ではSubBytes演算、ShiftRows演算、AddRoundKey演算を行った結果を出力する。

【０１２１】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部135は図１１記載の通りに暗号化処理を実行可能である。

【０１２２】

一方、鍵拡張部132は、鍵準備期間の後、実行鍵Ａ（162）からはwkey1、実行鍵Ｂ（163）からはwkey0を出力している。したがって、暗号化処理の開始時（T17）において、ラウンド処理部135に対してwkey0およびwkey1が供給されている。鍵拡張部132は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey1を用いてwkey2を生成し、実行鍵Ａレジスタに保持する。これによりT18において、ラウンド処理部135にはwkey2が供給される。以下、T26まで同様にして実行鍵

が供給されていく。T26においてwkey10を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部132は次なる暗号化処理の開始に備え、共通鍵152として外部より供給されつづけているwkey0を用いてwkey1を生成し、実行鍵Ａレジスタに保持する(T27)。

【０１２３】

上記のように鍵拡張部132が動作すると、ラウンド処理部135は各サイクルにおいて図１１記載の通りに実行鍵を使用することができる。

【０１２４】

本第２の実施形態の暗号化処理期間の動作は以上のようにして行われる。図１８のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には暗号化処理の間隔は任意の長さとすればよい。

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０１２５】

続いて、本実施形態の復号処理の動作について説明する。図１９は本実施形態の復号処理時のタイミングチャートについて示したものである。図１９において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、…、T33とタイミング名が割り当てられている。同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図１４～図１７で使用されている信号線のナンバと一対一で対応している。

【０１２６】

図１９のタイミングチャートに示される復号処理時の動作も４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目、1ブロック目の復号処理期間（T17～T27）、そして、４つ目は、2ブロック目の復号処理期間（T27以降）である。

【０１２７】

パラメータ設定期間の役割、開始条件、終了条件は第１の実施形態と同様である。また、鍵準備期間はT06～T17までであり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。ただし、タイミングT16における鍵拡張部132の動作、およびタイミングT17における鍵拡張部132と制御部134の動作には、第１の実施形態とは異なる点があるので、それについて述べる。

【０１２８】

タイミングT16において、鍵拡張部132は実行鍵Ｂ（163）よりwkey0を出力する。ただし、wkey10は鍵拡張部132の内部に設けられたレジスタに保持されている。

【０１２９】

タイミングT17において、鍵拡張部132は実行鍵Ａ（162）よりwkey10を出力する。また、制御部134は選択信号170をAssertする。

【０１３０】

1ブロック目の復号処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０１３１】

制御部134は選択信号170を復号処理の終了時にAssertし、復号処理の１サイクル目(T18,T28)にNegateする。そして、選択信号175を復号処理の最終サイクル（T16）でAssertし、復号処理の終了時（T17）にNegateする。さらに、選択信号171を復号処理の１サイクル目にAssertし、復号処理の終了時にNegateする。

【０１３２】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ118は選択信号170がNegateされている時はInvMixColumns演算部116の出力、Assertされている時はAddRoundKey演算部121の出力を選択し出力する。また、セレクタ138は選択信号175がNegateされている時はInvSubBytes演算部120の出力、Assertされている時はAddRoundKey演算部117の出力を選択し出力する。

【０１３３】

したがって、ラウンド処理部136は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、InvShiftRows演算、InvSubBytes演算を行う。1サイクル目からは1サイクル前の結果に対して、AddRoundKey演算、InvMixColumns演算、InvShiftRows演算、InvSubBytes演算を行った結果を出力する。そして、9サイクル目（T26～T27）ではAddRoundKey演算、InvMixColumns演算、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算を行った結果を出力する。

【０１３４】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部136は図１１記載の通りに復号処理を実行可能である。

【０１３５】

一方、鍵拡張部132は、鍵準備期間の後、実行鍵Ａ（162）からはwkey10、実行鍵Ｂ（163）からはwkey0を出力している。したがって、復号処理の開始時（T17）において、ラウンド処理部136に対してwkey10が供給されている。鍵拡張部132は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey10を用いてwkey9を生成し、実行鍵Ａレジスタに保持する。これによりT18において、ラウンド処理部136にはwkey9が供給される。以下、T26まで同様にして実行鍵が供給されていく。T26においてwkey1を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部132は次なる復号処理の開始に備え、鍵拡張部の内部レジスタに保持されているwkey10を実行鍵Ａレジスタにロードする(T27)。

【０１３６】

上記のように鍵拡張部132が動作すると、ラウンド処理部136は各サイクルにおいて図１１記載の通りに実行鍵を使用することができる。

【０１３７】

本第２の実施形態の復号処理期間の動作は以上のようにして行われる。図１９のタイミングチャートでは1ブロック目の復号処理の終了後、2ブロック目の復号処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの復号処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には復号処理の間隔は任意の長さとすればよい。

【０１３８】

あらかじめ決められたブロック数の復号処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０１３９】

第２の実施形態は以上のようにして実施可能である。本第２の実施形態は１サイクル内で実行しなければならない処理の処理時間の最大値をわずかに増やすものの、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０１４０】

以上の第２の実施形態はあくまで本発明の一例に過ぎず、本発明の効果は上記実施形態に限ったことではない。

【０１４１】

＜第３の実施形態＞

図２０は第３の実施形態において各クロックサイクル内で実行される暗号化処理、復号処理の処理内容を示した図である。同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。

【０１４２】

本第３の実施形態の暗号化処理は、0サイクル目では、AddRoundKey演算、ShiftRows演算、SubBytes演算を実行する。そして、１サイクル目から８サイクル目ではAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算を実行する。そして、９サイクル目では、MixColumns演算、第１のAddRoundKey演算、SubBytes演算、ShiftRows演算、第２のAddRoundKey演算を実行する。実行鍵は0サイクル目ではwkey0、1サイクル目ではwkey1、…、８サイクル目ではwkey8、９サイクル目では２つの実行鍵とwkey9およびwkey10が用いられる。

【０１４３】

本第３の実施形態がトータルで実行している処理は従来例と同じであるが、本第３の実施形態ではAESの暗号化処理を1つ少ないクロックサイクル数で実行することができる。

【０１４４】

次に、本第３の実施形態において各クロックサイクル内で実行される処理に必要な処理時間について述べる。図２１は、第３の実施形態において各クロックサイクル内に実行される暗号化処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第３の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図２１に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。

【０１４５】

本第３の実施形態では、第１のAddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算、および第２のAddRoundKey演算を行う９サイクル目の処理に必要な処理時間は、AddRoundKey演算、SubBytes演算、ShiftRows演算、およびMixColumns演算を行う１～８サイクル目の処理に必要な処理時間や、AddRoundKey演算、SubBytes演算、ShiftRows演算を行う０サイクル目の処理に必要な処理時間よりも長い。したがって、本第３の実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。

【０１４６】

本発明はAESの復号処理についても同様に適用可能である。

【０１４７】

図２０に示すように、本第３の実施形態の復号処理は、0サイクル目では、第１のAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、InvMixColumns演算、および第２のAddRoundKey演算を実行する。そして、１サイクル目から８サイクル目ではAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、およびInvMixColumns演算を実行する。そして、９サイクル目ではAddRoundKey演算、InvShiftRows演算、およびInvSubBytes演算を実行する。実行鍵は0サイクル目ではwkey10およびwkey9、１サイクル目ではwkey8、…、９サイクル目ではwkey0が用いられる。

【０１４８】

本第３の実施形態がトータルで実行している処理は従来と同じであるが、本実施形態ではAESの復号処理を1つ少ないクロックサイクル数で実行することができる。

【０１４９】

次に、本第３の実施形態において各クロックサイクル内に実行される復号処理に必要な処理時間について述べる。図２２は、第３の実施形態において各クロックサイクル内で実

行される復号処理に必要な処理時間を比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図２２に示すように、各サブブロック演算の処理時間は、InvSubBytes演算がもっとも長く、次いでInvMixColumns演算、AddRoundKey演算、InvShiftRows演算である。

【０１５０】

本第３の実施形態では、第１のAddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算、第２のAddRoundKey演算を行う０サイクル目の処理に必要な処理時間は、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行う１～８サイクル目の処理に必要な処理時間や、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算を行う９サイクル目の処理に必要な処理時間よりも長い。したがって、本第３の実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。

【０１５１】

ここまでで説明してきた本第３の実施形態の特徴についてまとめる。

【０１５２】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、10サイクル目と0サイクル目に実行される処理に必要な処理時間を合わせても、１～９サイクル目に実行される処理に必要な処理時間に及ばないというように、1サイクル内で実行される処理に必要な処理時間にばらつきがあった。

【０１５３】

一方、本第３の実施形態では1サイクル内で実行される処理に必要な処理時間を均等にするよう暗号化処理、復号処理の処理の区切りを変更した。

【０１５４】

本第３の実施形態は1サイクル内で実行される処理に必要な処理時間の最大値をわずかに増やすため、従来技術が実施可能な条件下で必ずしも本実施形態が実施可能であるとは限らない。しかし、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理および復号処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０１５５】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。図２３は、本実施形態のAES処理回路のブロック図を示したものである。図２３において、141はAESの処理を実行するAES処理回路である。142は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。143は鍵拡張部142より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。144はAES処理回路141の外部からの制御信号を受け、鍵拡張部142および暗号化・復号処理部143の動作を制御するための信号を生成し、かつAES処理回路141の外部に対して動作完了を通知するための信号を生成する制御部である。

【０１５６】

なお、同図において第１の実施形態および第２の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略する。

【０１５７】
次に、暗号化・復号処理部143について説明する。図２４は暗号化・復号処理部143のブロック図について示したものである。同図において、145は、選択信号170および選択信号175による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて1サイクル分の暗号化処理を行うラウンド処理部である。146は選択信号170および選択信号175による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて復号処理を行うラウンド処理部である。
【０１５８】
上記構成において、暗号化・復号処理部143のセレクタ109は、選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。
【０１５９】
なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略する。
【０１６０】
次に、ラウンド処理部145について説明する。図２５はラウンド処理部145のブロック図について示したものである。同図において、113は入力信号165を入力とし、MixColumns演算を行うところのMixColumns演算部である。137は選択信号175に応じて入力信号165とMixColumns演算部113の出力のいずれか一方を選択し出力するセレクタである。110はセレクタ137の出力および実行鍵Ａ（162）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。111はAddRondKey演算部110の出力を入力としSubBytes演算を行うところのSubBytes演算部である。112はSubBytes演算部111の出力を入力としShiftRows演算を行うところのShiftRows演算部である。114はShiftRows演算部112の出力および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。115は選択信号170に応じてShiftRows演算部112の出力とAddRoundKey演算部114の出力のいずれか一方を選択し出力するセレクタである。セレクタ115の出力信号はラウンド処理部145の出力となる。
【０１６１】
上記構成において、セレクタ115は選択信号170がNegateされている時はShiftRows演算部112の出力、Assertされている時はAddRoundKey演算部114の出力を選択し、出力する。セレクタ137は選択信号175がNegateされている時はMixColumns演算部113の出力、Assertされている時は入力信号165を選択し出力する。
【０１６２】
次に、ラウンド処理部146について説明する。図２６はラウンド処理部146のブロック図について示したものである。同図において、121は入力信号165および実行鍵Ａ（162）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。118は選択信号170に応じて入力信号165とAddRoundKey演算部121の出力のいずれか一方を選択し出力するセレクタである。119はセレクタ118の出力を入力としInvShiftRows演算を行うところのInvShiftRows演算部である。120はInvShiftRows演算部119の出力を入力としInvSubBytes演算を行うところのInvSubBytes演算部である。117はInvSubBytes演算部120および実行鍵Ｂ（163）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。116はAddRoundKey演算部117の出力を入力としInvMixColumns演算を行うところのInvMixColumns演算部である。138は選択信号175に応じて、InvMixColumns演算部116の出力かAddRoundKey演算部117の出力のいずれか一方を選択し、出力するセレクタである。セレクタ138の出力はラウンド処理部146の出力となる。
【０１６３】
上記構成において、セレクタ118は選択信号170がNegateされている時は入力信号165、Assertされている時はAddRoundKey演算部121の出力を選択し出力する。セレクタ138は選択信号175がNegateされている時はInvMixColumns演算部116、Assertされている時はAddRoundKey演算部117の出力を選択し出力する。
【０１６４】

次に、上記構成における暗号化処理時の動作について説明する。図２７は本実施形態における暗号化処理時のタイミングチャートについて示したものである。図２７において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、…、T33とタイミング名が割り当てられている。同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図２３～図２６で使用されている信号線のナンバと一対一で対応している。図２７のタイミングチャートに示される暗号化処理時の動作は、４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の暗号化処理期間（T17～T27）、そして４つ目は、2ブロック目の暗号化処理期間（T27以降）である。

【０１６５】

パラメータ設定期間の役割、開始条件、終了条件は第１の実施形態と同様である。また、鍵準備期間はT06～T17までであり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。ただし、制御部144は鍵準備期間が終了時（T17）に選択信号175をAssertする。

【０１６６】

1ブロック目の暗号化処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０１６７】

制御部144は選択信号175を暗号化処理の終了時にAssertし、暗号化処理の１サイクル目(T18,T28)にNegateする。そして、選択信号170を暗号化処理の最終サイクル（T16）でAssertし、暗号化処理の終了時（T17）にNegateする。さらに、選択信号171を暗号化処理の１サイクル目にAssertし、暗号化処理の終了時にNegateする。

【０１６８】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ115は選択信号170がNegateされている時はShiftRows演算部112の出力、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。また、セレクタ137は選択信号175がNegateされている時はMixColumns演算部113の出力、Assertされている時は入力信号165を選択し出力する。

【０１６９】

したがって、ラウンド処理部145は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、SubBytes演算、ShiftRows演算を行う。1サイクル目からは1サイクル時間前の結果に対して、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行った結果を出力する。そして、9サイクル目（T26～T27）ではMixColumns演算、AddRoundKey演算、SubBytes演算、ShiftRows演算、AddRoundKey演算を行った結果を出力する。

【０１７０】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部145は図２０記載の通りに暗号化処理を実行可能である。

【０１７１】

一方、鍵拡張部142は、鍵準備期間の後、実行鍵Ａ（162）からはwkey0、実行鍵Ｂ（163）からはwkey10を出力している。したがって、暗号化処理の開始時（T17）において、ラウンド処理部145に対してwkey0が供給されている。鍵拡張部142は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey0を用いてwkey1を生成し、実行鍵Ａレジスタに保持する。これによりタイミングT18において、ラウンド処理部145にはwkey1が供給される。以下、T26まで同様にして実行鍵が供給されていく。T26では実行鍵Ｂ（163）のwkey10もあわせて供給される。T26においてwkey10を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部142

は次なる暗号化処理の開始に備え、共通鍵152として外部より供給されつづけているwkey0を実行鍵Ａレジスタに保持する(T27)。

【０１７２】

上記のように鍵拡張部142が動作すると、ラウンド処理部145は各サイクルにおいて図２０記載の通りに実行鍵を使用することができる。

【０１７３】

本第３の実施形態の暗号化処理期間の動作は以上のようにして行われる。図２７のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には暗号化処理の間隔は任意の長さとすればよい。

【０１７４】

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０１７５】

続いて、本実施形態の復号処理の動作について説明する。図２８は本実施形態の復号処理時のタイミングチャートについて示したものである。図２８において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、…、T33とタイミング名が割り当てられている。同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図２３～図２６で使用されている信号線のナンバと一対一で対応している。

【０１７６】

図２８のタイミングチャートに示される復号処理時の動作は、４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の復号処理期間（T17～T27）、そして、４つ目は2ブロック目の復号処理期間（T27以降）である。

【０１７７】

パラメータ設定期間の役割、開始条件、終了条件は第１の実施形態と同様である。また、鍵準備期間はT06～T17までであり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。ただし、鍵準備期間の終了時（T17）に制御部144は選択信号170をAssertする。

【０１７８】

1ブロック目の復号処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０１７９】

制御部144は選択信号170を復号処理の終了時にAssertし、復号処理の１サイクル目(T18,T28)にNegateする。そして、選択信号175を復号処理の最終サイクル（T16）でAssertし、復号処理の終了時（T17）にNegateする。さらに、選択信号171を復号処理の１サイクル目にAssertし、復号処理の終了時にNegateする。

【０１８０】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ118は選択信号170がNegateされている時は入力信号165、Assertされている時はAddRoundKey演算部121の出力を選択し出力する。また、セレクタ138は選択信号175がNegateされている時はInvMixColumns演算部116の出力、Assertされている時はAddRoundKey演算部117の出力を選択し出力する。

【０１８１】

したがって、ラウンド処理部146は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算、InvMixC

olumns演算を行う。1サイクル目からは1サイクル前の結果に対して、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算、InvMixColumns演算を行った結果を出力する。また、9サイクル目（T26～T27）では、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算を行った結果を出力する。

【０１８２】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部146は図２０に記載された通りに復号処理を実行可能である。

【０１８３】

一方、鍵拡張部142は、鍵準備期間の後、実行鍵Ａ（162）からはwkey9、実行鍵Ｂ（163）からはwkey10を出力している。したがって、復号処理の開始時（T17）において、ラウンド処理部146に対してwkey10およびwkey9が供給されている。鍵拡張部142は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey9を用いてwkey8を生成し、実行鍵Ａレジスタに保持する。これによりT18において、ラウンド処理部146にはwkey8が供給される。以下、T26まで同様にして実行鍵が供給されていく。T26においてwkey0を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部142は次なる復号処理の開始に備え、実行鍵Ｂレジスタに保持されているwkey10を用いてwkey9を生成し、実行鍵Ａレジスタに保持する(T27)。

【０１８４】

上記のように鍵拡張部142が動作すると、ラウンド処理部146は各サイクルにおいて図２０記載の通りに実行鍵を使用することができる。

【０１８５】

本実施形態の復号処理期間の動作は以上のようにして行われる。図２８のタイミングチャートでは1ブロック目の復号処理の終了後、2ブロック目の復号処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの復号処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には復号処理の間隔は任意の長さとすればよい。

【０１８６】

あらかじめ決められたブロック数の復号処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０１８７】

本第３の実施形態は以上のようにして実施可能である。本第３の実施形態は１サイクル内で実行しなければならない処理の処理時間の最大値をわずかに増やすものの、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理および復号処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０１８８】

以上説明したように、本発明の考え方を応用することで、基本となる第１の実施形態以外にも多数の実施形態を得ることができる。第２の実施形態および第３の実施形態はその一例である。他にも、図６２のような8サイクル目でAddRoundKeyを２回実行する構成のように、暗号化処理の任意のサイクルでAddRoundKeyを2回実行する構成も考えられる。実施形態はあくまで本発明の一例に過ぎず、本発明の効果は上記実施形態の記載に限ったことではない。

【０１８９】

＜第４の実施形態＞

本第４の実施形態はFIPS197記載のEquivalent Inverse Cipherを用いて復号処理を行う際の実施例を示すものである。

【０１９０】

図２９は第４の実施形態において各クロックサイクル内に実行される暗号化処理の処理内容を従来例と比較して示したものである。

【０１９１】
同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。
【０１９２】
本実施形態は、０サイクル目から８サイクル目ではAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算を実行する。そして、９サイクル目では、第１のAddRoundKey演算、ShiftRows演算、SubBytes演算、第２のAddRoundKey演算を実行する。実行鍵は0サイクル目ではwkey0、1サイクル目ではwkey1、…、８サイクル目ではwkey8が用いられ、9サイクル目では２つの実行鍵wkey9、wkey10が必要となる。
【０１９３】
本第４の実施形態は従来技術とトータルで実行している処理は同じであるが、本第４の実施形態ではAESの暗号化処理を1つ少ないクロックサイクル数で実行することができる。
【０１９４】
次に、本第４の実施形態において各クロックサイクル内に実行される暗号化処理に必要な処理時間について述べる。図３１は、第４の実施形態において各クロックサイクル内に実行される暗号化処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第４の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図３１に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。
【０１９５】
本第４の実施形態では、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行う０～８サイクル目の処理に必要な処理時間は、第１のAddRoundKey演算、SubBytes演算、ShiftRows演算、第２のAddRoundKey演算を行う9サイクル目の処理に必要な処理時間よりも長い。したがって、本第４の実施形態において1サイクル内で実行される処理に必要な処理時間の最大値を従来技術のものと比較すると、両者は等しい。従来技術において1サイクル内で実行される処理に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態もまた実施可能である。
【０１９６】
本発明はAESの復号処理についても同様に適用可能である。
【０１９７】
図３０は第４の実施形態において各クロックサイクル内で実行される復号処理の処理内容を従来技術と比較して示した図である。
【０１９８】
同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数を示すものである。また、特殊実行鍵wkeyi’（iはラウンド数を示す）はFIPS197記載のEquivalent Inverse Cipherに必要なとなるRound Keyのことを指すものとする。
【０１９９】
本第４の実施形態は、０サイクル目から８サイクル目ではAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、InvMixColumns演算を実行する。そして、９サイクル目では第１のAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、第２のAddRoundKey演算を実行する。実行鍵は0サイクル目ではwkey10、1サイクル目ではwkey9’、…、８サイクル目ではwkey2’が用いられ、9サイクル目では２つの実行鍵wkey1’、wkey0が必要となる。
【０２００】
本第４の実施形態は従来技術とトータルで実行している処理は同じであるが、本第４の実施形態ではAESの復号処理を1つ少ないクロックサイクル数で実行することができる。
【０２０１】
次に、本第４の実施形態において各クロックサイクル内で実行される復号処理に必要な

処理時間について述べる。図３１は、第４の実施形態において各クロックサイクル内で実行される復号処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図３１に示すように、各サブブロック演算の処理時間は、InvSubBytes演算がもっとも長く、次いでInvMixColumns演算、AddRoundKey演算、InvShiftRows演算である。

【０２０２】

本第４の実施形態では、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行う０～８サイクル目の処理に必要な処理時間は、第１のAddRoundKey演算、InvSubBytes演算、InvShiftRows演算、第２のAddRoundKey演算を行う９サイクル目の処理に必要な処理時間よりも長い。したがって、本実施形態において1サイクル内で実行される処理に必要な処理時間の最大値を従来技術のものと比較すると、両者は等しい。従来技術において1サイクル内で実行される処理に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態もまた実施可能である。

【０２０３】

ここまでで説明してきた本第４の実施形態の特徴についてまとめる。

【０２０４】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、10サイクル目と0サイクル目に実行される処理に必要な処理時間を合わせても、１～９サイクル目に実行される処理に必要な処理時間に及ばないというように、1サイクル内で実行される処理に必要な処理時間にばらつきがあった。

【０２０５】

一方、本第４の実施形態では1サイクル内で実行される処理に必要な処理時間を均等にするよう暗号化処理、復号処理の処理の区切りを変更した。本発明は1サイクル内に実行される処理に必要な処理時間を増やすことなく、AESの暗号化処理、復号処理に要するクロックサイクル数を1サイクル削減しており、これにより約10%程度の処理速度の向上が得られる。

【０２０６】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。

【０２０７】

図３２は、本第４の実施形態のAES処理回路のブロック図を示したものである。

【０２０８】

図３２において、201はAESの処理を実行するAES処理回路である。202は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。203は鍵拡張部202より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。204はAES処理回路201の外部からの制御信号を受け、鍵拡張部202および暗号化・復号処理部203の動作を制御するための信号を生成し、かつAES処理回路201の外部に対して動作完了を通知するための信号を生成する制御部である。

【０２０９】

なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略する。

【０２１０】

次に、暗号化・復号処理部203について説明する。図３３は暗号化・復号処理部203のブロック図を示したものである。同図において、205は選択信号170、暗号化・復号処理選択信号153および選択信号175による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて1サイクル分の暗号化処理もしくは復号処理を行うラウンド処理部である。

【０２１１】

上記構成において、セレクタ109は、選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。

【０２１２】

なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略する。

【０２１３】

次に、ラウンド処理部205について説明する。図３４はラウンド処理部205のブロック図を示したものである。同図において、110は入力信号165および実行鍵Ａ（162）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。222はAddRoundKey演算部110の出力を入力とし暗号化・復号処理選択信号153に応じてSubBytes演算とInvSubBytes演算のいずれかを行うところのSubBytes/InvSubBytes演算部である。223はSubBytes/InvSubBytes演算部222の出力を入力とし暗号化・復号処理選択信号153に応じてShiftRows演算とInvShiftRows演算の一方を行うところのShiftRows/InvShiftRows演算部である。224はShiftRows/InvShiftRows演算部223の出力を入力とし暗号化・復号処理選択信号153に応じてMixColumns演算とInvMixColumns演算の一方を行うところのMixColumns/InvMixColumns演算部である。114はShiftRows/InvShiftRows演算部223の出力を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。115は選択信号170に応じてMixColumns/InvMixColumns演算部224の出力とAddRoundKey演算部114の出力のいずれか一方を選択し出力するセレクタである。セレクタ115の出力信号はラウンド処理部205の出力となる。

【０２１４】

上記構成において、セレクタ115は選択信号170がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。また、SubBytes/InvSubBytes演算部222、ShiftRows/InvShiftRows演算部223、およびMixColumns/InvMixColumns演算部224は、暗号化・復号処理選択信号153がNegateされている時はそれぞれSubBytes演算、ShiftRows演算部、MixColumns演算を行い、暗号化・復号処理選択信号153がAssertされている時はそれぞれInvSubBytes演算、InvShiftRows演算部、InvMixColumns演算を行う。

【０２１５】

次に、上記構成における暗号化処理時の動作を図９のタイミングチャートに従って説明する。図９において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、・・・、T33とタイミング名が割り当てられている。

【０２１６】

同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図３２～図３４で使用されている信号線のナンバと一対一で対応している。

【０２１７】

図９のタイミングチャートに示される暗号化処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の暗号化処理期間（T17～T27）、そして、４つ目は2ブロック目の暗号化処理期間（T27以降）である。

【０２１８】

パラメータ設定期間の役割、開始条件、終了条件は第１の実施形態と同様である。また、鍵準備期間はT06～T17までである。鍵準備期間の開始条件、終了条件、各回路の動作は第１の実施形態の説明とまったく同様であるため、ここでは省略する。

【０２１９】

1ブロック目の暗号化処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０２２０】

制御部204は選択信号170を暗号化処理の最終サイクル（T16）でAssertし、暗号化処理

の終了時（T17）にNegateする。さらに、選択信号171を暗号化処理の１サイクル目にAssertし、暗号化処理の終了時にNegateする。

【０２２１】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ115は選択信号170がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。また、SubBytes/InvSubBytes演算部222、ShiftRows/InvShiftRows演算部223、およびMixColumns/InvMixColumns演算部224は、暗号化・復号処理選択信号153がNegateされている時はそれぞれSubBytes演算、ShiftRows演算部、MixColumns演算を行い、暗号化・復号処理選択信号153がAssertされている時はそれぞれInvSubBytes演算、InvShiftRows演算部、InvMixColumns演算を行う。

【０２２２】

したがって、ラウンド処理部205は、０サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行う。1サイクル目からは1サイクル時間前の結果に対してAddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行った結果を出力する。そして、9サイクル目（T26～T27）では、AddRoundKey演算、SubBytes演算、ShiftRows演算、AddRoundKey演算を行った結果を出力する。

【０２２３】

選択信号171、選択信号170を先述のようにコントロールすることでラウンド処理部205は図２９記載の通りに暗号化処理を実行可能である。

【０２２４】

一方、鍵拡張部202は、鍵準備期間の後、実行鍵Ａ（162）からはwkey0、実行鍵Ｂ（163）からはwkey10を出力している。したがって、暗号化処理の開始時（T17）において、ラウンド処理部205に対してwkey0が供給されている。鍵拡張部202は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey0を用いてwkey1を生成し、実行鍵Ａレジスタに保持する。これによりタイミングT18において、ラウンド処理部205にはwkey1が供給される。以下、タイミングT26まで同様にして実行鍵が供給されていく。T26では実行鍵Ｂ（163）もあわせ2つの実行鍵wkey9とwkey10が供給される。T26においてwkey9を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部202は次なる暗号化処理の開始に備え、共通鍵152として外部より供給されつづけているwkey0を実行鍵Ａレジスタに保持する(T27)。

【０２２５】

上記のように鍵拡張部202が動作すると、ラウンド処理部205は各サイクルにおいて図２９記載の通りに実行鍵を使用することができる。

【０２２６】

本第４の実施形態の暗号化処理期間の動作は以上のようにして行われる。図９のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には暗号化処理の間隔は任意の長さとすればよい。

【０２２７】

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０２２８】

続いて、本実施形態の復号処理の動作について説明する。図３５は本第４の実施形態の復号処理時のタイミングチャートを示したものである。図３５において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、・・・、T33とタイミング名が割り当てられている。同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、

図３２～図３４で使用されている信号線のナンバと一対一で対応している。

【０２２９】

図３５のタイミングチャートに示される復号処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の復号処理期間（T17～T27）、そして、４つ目は2ブロック目の復号処理期間（T27以降）である。

【０２３０】

パラメータ設定期間の役割、開始条件、終了条件は第１の実施形態の暗号化処理時と同様である。

【０２３１】

鍵準備期間はT06～T17までであり、開始条件および終了条件は本第１の実施形態の暗号化処理時と同様である。各回路の動作も本実施形態の暗号化処理時とほぼ同様である。ただし、タイミングT16における鍵拡張部202の動作、およびタイミングT17における鍵拡張部202と制御部204の動作に、暗号化時とは異なる点があるので、それについて述べる。

【０２３２】

タイミングT16において、鍵拡張部202は実行鍵Ｂ（163）よりwkey0を出力し、実行鍵Ａ（162）よりwkey10を出力する。ただし、wkey10は鍵拡張部202の内部に設けられたレジスタにも別途保持されている。そして、鍵拡張部202はT16においてwkey10から逆順に鍵拡張を行い、特殊実行鍵をwkey9’を生成する。

【０２３３】

タイミングT17において、鍵拡張部202は実行鍵Ａ（162）よりwkey9’を出力する。また、制御部204は選択信号170をAssertする。

【０２３４】

1ブロック目の復号処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０２３５】

制御部204は選択信号170を復号処理の最終サイクル（T16）でAssertし、復号処理の終了時（T17）にNegateする。そして、選択信号171を復号処理の１サイクル目にAssertし、復号処理の終了時にNegateする。

【０２３６】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ115は選択信号170がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。また、SubBytes/InvSubBytes演算部222、ShiftRows/InvShiftRows演算部223、およびMixColumns/InvMixColumns演算部224は、暗号化・復号処理選択信号153がNegateされている時はそれぞれSubBytes演算、ShiftRows演算部、MixColumns演算を行い、暗号化・復号処理選択信号153がAssertされている時はそれぞれInvSubBytes演算、InvShiftRows演算部、InvMixColumns演算を行う。

【０２３７】

したがって、ラウンド処理部205は、０サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行う。1サイクル目からは1サイクル時間前の結果に対してAddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行った結果を出力する。また、9サイクル目（T26～T27）では、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、AddRoundKey演算を行った結果を出力する。

【０２３８】

選択信号171、選択信号170を先述のようにコントロールすることでラウンド処理部205

は図３０に示した通りに復号処理を実行可能である。

【０２３９】

一方、鍵拡張部202は、鍵準備期間の後、実行鍵Ａ（162）からはwkey10、実行鍵Ｂ（163）からはwkey0を出力している。したがって、復号処理の開始時（T17）において、ラウンド処理部205に対してwkey10が供給されている。鍵拡張部202は、暗号化・復号処理開始信号158より復号処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey10を用いてwkey9’を生成し、実行鍵Ａレジスタに保持する。これによりタイミングT18において、ラウンド処理部205にはwkey9’が供給される。以下、タイミングT26まで同様にして実行鍵が供給されていく。タイミングT26では実行鍵Ｂ（163）もあわせ2つの実行鍵wkey1’とwkey0が供給される。タイミングT26においてwkey1’を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部202は次なる復号処理の開始に備え、鍵拡張部の内部レジスタに保持されているwkey10を実行鍵Ａレジスタにロードする(T27)。

【０２４０】

上記のように鍵拡張部202が動作すると、ラウンド処理部205は各サイクルにおいて図３０に示した通りに実行鍵を使用することができる。

【０２４１】

本第４の実施形態の復号処理期間の動作は以上のようにして行われる。図３５のタイミングチャートでは1ブロック目の復号処理の終了後、2ブロック目の復号処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの復号処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には復号処理の間隔は任意の長さとすればよい。

【０２４２】

あらかじめ決められたブロック数の復号処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０２４３】

本第４の実施形態は以上のようにして実施可能である。本第４の実施形態は、Equivalent Inverse Cipherを用いて復号を行う際の回路構成およびその動作について示したものである。本第４の実施形態は１サイクル内で実行しなければならない処理の処理時間の最大値を増やすことなくAESの暗号化処理に要するクロックサイクル数を1サイクル削減することができる。これにより約10%程度の処理速度の向上が得られる。

【０２４４】

以上説明した第４の実施形態はあくまで本発明の一例に過ぎず、本発明の効果は上記実施形態に限ったことではない。

【０２４５】

＜第５の実施形態＞

本第５の実施形態はFIPS197記載のEquivalent Inverse Cipherを用いて復号処理を行う例を示す。

【０２４６】

図３６は第５の実施形態において各クロックサイクル内で実行される暗号化処理、復号処理の処理内容を示した図である。

【０２４７】

同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。

【０２４８】

本第５の実施形態の暗号化処理は、0サイクル目では2つの実行鍵を用いて、第１のAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算、第２のAddRoundKey演算を実行する。そして、１サイクル目から８サイクル目ではAddRoundKey演算、ShiftRows演算、SubBytes演算、MixColumns演算を実行する。そして、９サイクル目では、AddRoundKey演算、ShiftRows演算、SubBytes演算を実行する。実行鍵は0サイクル目ではwkey0とwkey

1、1サイクル目ではwkey2、…、９サイクル目ではwkey10が用いられる。

【０２４９】

本第５の実施形態がトータルで実行している処理は従来と同じであるが、本実施形態ではAESの暗号化処理を1つ少ないクロックサイクル数で実行することができる。

【０２５０】

次に、本第５の実施形態において各クロックサイクル内で実行される暗号化処理に必要な処理時間について述べる。図３７は、第５の実施形態において各クロックサイクル内で実行される処理に必要な処理時間を比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第５の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図３７に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。

【０２５１】

本第５の実施形態では、第１のAddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算、第２のAddRoundKey演算を行う０サイクル目の処理必要な処理時間は、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行う１～８サイクル目の処理に必要な処理時間や、AddRoundKey演算、SubBytes演算、ShiftRows演算を行う９サイクル目の処理に必要な処理時間よりも長い。したがって、本第５の実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。

【０２５２】

本発明はAESの復号処理についても同様に適用可能である。

【０２５３】

図３６に示すように、本実施形態の復号処理は、0サイクル目では第１のAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、InvMixColumns演算、第２のAddRoundKey演算を実行する。そして、１サイクル目から８サイクル目ではAddRoundKey演算、InvShiftRows演算、InvSubBytes演算、InvMixColumns演算を実行する。そして、９サイクル目ではAddRoundKey演算、InvShiftRows演算、InvSubBytes演算を実行する。実行鍵は0サイクル目ではwkey10およびwkey9’、１サイクル目ではwkey8’、…、９サイクル目ではwkey0が用いられる。

【０２５４】

本第５の実施形態がトータルで実行している処理は従来の実施例と同じであるが、本第５の実施形態ではAESの復号処理を1つ少ないクロックサイクル数で実行することができる。

【０２５５】

次に、本第５の実施形態において各クロックサイクル内で実行される復号処理に必要な処理時間について述べる。図３７は、第５の実施形態において各クロックサイクル内で実行される復号処理に必要な処理時間を従来技術のものと比較した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図３７に示すように、各サブブロック演算の処理時間は、InvSubBytes演算がもっとも長く、次いでInvMixColumns演算、AddRoundKey演算、InvShiftRows演算である。

【０２５６】

本第５の実施形態では、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算、AddRoundKey演算を行う０サイクル目の処理に必要な処理時間は、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算、InvMixColumns演算を行う１～８サイ

クル目の処理に必要な処理時間や、AddRoundKey演算、InvSubBytes演算、InvShiftRows演算を行う９サイクル目の処理に必要な処理時間よりも長い。したがって、本第５の実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。

【０２５７】

ここまでで説明してきた本第５の実施形態の特徴についてまとめる。

【０２５８】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、10サイクル目と0サイクル目に実行される処理に必要な処理時間を合わせても、１～９サイクル目に実行される処理に必要な処理時間に及ばないというように、1サイクル内で実行される処理に必要な処理時間にばらつきがあった。

【０２５９】

一方、本第５の実施形態では1サイクル内で実行される処理に必要な処理時間を均等にするよう暗号化処理、復号処理の処理の区切りを変更した。

【０２６０】

本第５の実施形態は1サイクル内で実行される処理に必要な処理時間の最大値をわずかに増やすため、従来技術が実施可能な条件下で必ずしも本実施形態が実施可能であるとは限らない。しかし、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理および復号処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０２６１】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。

【０２６２】

図３８は本第５の実施形態のAES処理回路のブロック図を示したものである。図３８において、231はAESの処理を実行するAES処理回路である。232は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。233は鍵拡張部232より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。234はAES処理回路231の外部からの制御信号を受け、鍵拡張部232および暗号化・復号処理部233の動作を制御するための信号を生成し、かつAES処理回路231の外部に対して動作完了を通知するための信号を生成する制御部である。

【０２６３】

なお、同図において第１の実施形態および第２の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略する。

【０２６４】

次に、暗号化・復号処理部233について説明する。図３９は暗号化・復号処理部233のブロック図について示したものである。同図において、235は選択信号170、選択信号175および暗号化・復号処理選択信号153による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて1サイクル分の暗号化処理もしくは復号処理を行うラウンド処理部である。

【０２６５】

上記構成において、暗号化・復号処理部233のセレクタ109は、選択信号171がNegateさ

れている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。

【０２６６】

なお、同図において第１の実施形態および第２の実施形態で説明した構成要素および信号線と同一のものに関しては、同じであるものとし、その説明を省略する。

【０２６７】

次に、ラウンド処理部235について説明する。図４０はラウンド処理部235のブロック図について示したものである。同図において、114は入力信号165および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。137は選択信号175に応じて入力信号165とAddRoundKey演算部114の出力のいずれか一方を選択し出力するセレクタである。222はセレクタ137の出力を入力とし暗号化・復号処理選択信号153に応じてSubBytes演算とInvSubBytes演算のいずれかを行うところのSubBytes/InvSubBytes演算部である。223はSubBytes/InvSubBytes演算部222の出力を入力とし暗号化・復号処理選択信号153に応じてShiftRows演算とInvShiftRows演算の一方を行うところのShiftRows/InvShiftRows演算部である。224はShiftRows/InvShiftRows演算部223の出力を入力とし暗号化・復号処理選択信号153に応じてMixColumns演算とInvMixColumns演算の一方を行うところのMixColumns/InvMixColumns演算部である。115は選択信号170に応じてMixColumns/InvMixColumns演算部224の出力とShiftRows/InvShiftRows演算部223の出力のいずれか一方を選択し出力するセレクタである。110はセレクタ115の出力および実行鍵Ａ（162）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。AddRoundKey演算部110の出力信号はラウンド処理部235の出力となる。

【０２６８】

上記構成において、セレクタ115は選択信号170がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時はShiftRows/InvShiftRows演算部223の出力を選択し出力する。セレクタ137は選択信号175がNegateされている時は入力信号165、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。

【０２６９】

次に、上記構成における暗号化処理時の動作を図１８のタイミングチャートに従って説明する。同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図３８～図４０で使用されている信号線のナンバと一対一で対応している。

【０２７０】

図１８のタイミングチャートに示される暗号化処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の暗号化処理期間（T17～T27）であり、４つ目は、2ブロック目の暗号化処理期間（T27以降）である。

【０２７１】

パラメータ設定期間の役割、開始条件、終了条件は第２の実施形態と同様である。また、鍵準備期間はT06～T17までの期間である、開始条件、終了条件および各回路の動作も第２の実施形態と同様であるため説明を省略する。1ブロック目の暗号化処理期間はT17からT27までの期間であり、開始条件および終了条件は第２の実施形態と同様である。各回路の動作も第２の実施形態のものと同様である。

【０２７２】

制御部234は選択信号175を暗号化処理の終了時にAssertし、暗号化処理の１サイクル目(T18,T28)にNegateする。そして、選択信号170を暗号化処理の最終サイクル（T16）でAssertし、暗号化処理の終了時（T17）にNegateする。さらに、選択信号171を暗号化処理の１サイクル目にAssertし、暗号化処理の終了時にNegateする。

【０２７３】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ115は選択信号170がNegateされている時は入力信号165、Assertされている時はAdd

RoundKey演算部114の出力を選択し出力する。また、セレクタ137は選択信号175がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時はShiftRows/InvShiftRows演算部223の出力を選択し出力する。また、SubBytes/InvSubBytes演算部222、ShiftRows/InvShiftRows演算部223、およびMixColumns/InvMixColumns演算部224は、暗号化・復号処理選択信号153がNegateされている時はそれぞれSubBytes演算、ShiftRows演算部、MixColumns演算を行い、暗号化・復号処理選択信号153がAssertされている時はそれぞれInvSubBytes演算、InvShiftRows演算部、InvMixColumns演算を行う。

【０２７４】

したがって、ラウンド処理部235は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行う。1サイクル目からは1サイクル時間前の結果に対して、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行った結果を出力する。そして、9サイクル目（T26～T27）ではSubBytes演算、ShiftRows演算、AddRoundKey演算を行った結果を出力する。

【０２７５】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部235は図３６記載の通りに暗号化処理を実行可能である。

【０２７６】

一方、鍵拡張部232は、鍵準備期間の後、実行鍵Ａ（162）からはwkey1、実行鍵Ｂ（163）からはwkey0を出力している。したがって、暗号化処理の開始時（T17）において、ラウンド処理部235に対してwkey0およびwkey1が供給されている。鍵拡張部232は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey1を用いてwkey2を生成し、実行鍵Ａレジスタに保持する。これによりタイミングT18において、ラウンド処理部235にはwkey2が供給される。以下、タイミングT26まで同様にして実行鍵が供給されていく。タイミングT26においてwkey10を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部232は次なる暗号化処理の開始に備え、共通鍵152として外部より供給されつづけているwkey0を用いてwkey1を生成し、実行鍵Ａレジスタに保持する(T27)。

【０２７７】

上記のように鍵拡張部232が動作すると、ラウンド処理部235は各サイクルにおいて図３６に示した通りに実行鍵を使用することができる。

【０２７８】

本第５の実施形態の暗号化処理期間の動作は以上のようにして行われる。図１８のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には暗号化処理の間隔は任意の長さとすればよい。

【０２７９】

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０２８０】

続いて、本第５の実施形態の復号処理の動作について述べる。図４１は本第５の実施形態の復号処理のタイミングチャートを示したものである。図４１において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、・・・、T33とタイミング名が割り当てられている。

【０２８１】

同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図３８～図４０で使用されている信号線のナンバと一対一で対応している。

【０２８２】

図４１のタイミングチャートに示される復号処理時の動作は４つに大別される。１つ目

は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の復号処理期間（T17～T27）、そして、４つ目は2ブロック目の復号処理期間（T27以降）である。

【０２８３】

パラメータ設定期間の役割、開始条件、終了条件は本実施形態の暗号化処理時と同様である。ただし、復号処理時は暗号化・復号処理選択信号153はAssertされる。

【０２８４】

鍵準備期間はT06～T17までであり、開始条件および終了条件は本実施形態の暗号化処理時と同様である。各回路の動作も本実施形態の暗号化処理時とほぼ同様である。ただし、タイミングT16における鍵拡張部232の動作、およびタイミングT17における鍵拡張部232と制御部234の動作に、暗号化時とは異なる点があるので、それについて述べる。

【０２８５】

タイミングT16において、鍵拡張部232は実行鍵Ｂ（163）よりwkey10を出力し、実行鍵Ａ（162）からはwkey10を出力する。鍵拡張部232はタイミングT16においてwkey10から逆順に鍵拡張を行い、特殊実行鍵wkey9’を生成する。

【０２８６】

タイミングT17において、鍵拡張部232は実行鍵Ａ（162）よりwkey9’を出力する。また、制御部234は選択信号175をAssertする。

【０２８７】

鍵準備期間の終了時（T17）に制御部234は選択信号175をAssertする。

【０２８８】

1ブロック目の復号処理期間はT17からT27までの期間であり、開始条件および終了条件は第１の実施形態と同様である。各回路の動作も第１の実施形態のものとほぼ同様である。

【０２８９】

制御部234は選択信号170を復号処理の最終サイクル(T26)にAssertし、復号処理の１サイクル目(T18,T28)にNegateする。そして、選択信号175を復号処理の終了時（T17）でAssertし、復号処理の終了時（T17）にNegateする。さらに、選択信号171を復号処理の１サイクル目にAssertし、復号処理の終了時にNegateする。

【０２９０】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ137は選択信号175がNegateされている時は入力信号165、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。また、セレクタ115は選択信号170がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時はShiftRows/InvShiftRows演算部223の出力を選択し出力する。

【０２９１】

したがって、ラウンド処理部235は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算、InvMixColumns演算を行う。1サイクル目からは1サイクル前の結果に対して、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算、InvMixColumns演算を行った結果を出力する。また、9サイクル目（T26～T27）ではInvShiftRows演算、InvSubBytes演算、AddRoundKey演算を行った結果を出力する。

【０２９２】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部235は図３６に示した通りに復号処理を実行可能である。

【０２９３】

一方、鍵拡張部232は、鍵準備期間の後、実行鍵Ａ（162）からはwkey9’、実行鍵Ｂ（163）からはwkey10を出力している。したがって、復号処理の開始時（T17）において、ラ

ウンド処理部235に対してwkey10およびwkey9’が供給されている。鍵拡張部235は、暗号化・復号処理開始信号158より復号処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey9’を用いてwkey8’を生成し、実行鍵Ａレジスタに保持する。これによりT18において、ラウンド処理部235にはwkey8’が供給される。以下、タイミングT26まで同様にして実行鍵が供給されていく。タイミングT26においてwkey0を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部232は次なる復号処理の開始に備え、実行鍵Ｂレジスタに保持されているwkey10を用いてwkey9’を生成し、実行鍵Ａレジスタに保持する(T27)。

【０２９４】

上記のように鍵拡張部232が動作すると、ラウンド処理部235は各サイクルにおいて図３６に示した通りに実行鍵を使用することができる。

【０２９５】

本第５の実施形態の復号処理期間の動作は以上のようにして行われる。図４１のタイミングチャートでは1ブロック目の復号処理の終了後、2ブロック目の復号処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの復号処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には復号処理の間隔は任意の長さとすればよい。

【０２９６】

あらかじめ決められたブロック数の復号処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０２９７】

第５の実施形態は以上のようにして実施可能である。本第５の実施形態は１サイクル内で実行しなければならない処理の処理時間の最大値をわずかに増やすものの、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０２９８】

以上説明した第５の実施形態はあくまで本発明の一例に過ぎず、本発明の効果は上記実施形態に限ったことではない。

【０２９９】

＜第６の実施形態＞

本第６の実施形態はFIPS197記載のEquivalent Inverse Cipherを用いて復号処理を行う例を示す。

【０３００】

図４２は第６の実施形態において各クロックサイクル内で実行される暗号化処理、復号処理の処理内容を示した図である。

【０３０１】

同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。

【０３０２】

本第６の実施形態は、0サイクル目では2つの実行鍵を用いて、第１のAddRoundKey演算、SubBytes/InvSubBytes演算、ShiftRows/InvShiftRows演算、MixColumns/InvMixColumns演算、第２のAddRoundKey演算を実行する。そして、１サイクル目から８サイクル目ではSubBytes/InvSubBytes演算、ShiftRows/InvShiftRows演算、MixColumns/InvMixColumns演算、AddRoundKey演算を実行する。そして、９サイクル目ではSubBytes/InvSubBytes演算、ShiftRows/InvShiftRows演算、AddRoundKey演算を実行する。ただし、SubBytes/InvSubBytes演算とは、暗号化時はSubBytes演算、復号時はInvSubBytes演算を実行することを表し、ShiftRows/InvShiftRows演算とは、暗号化時はShiftRows演算、復号時はInvShiftRows演算を実行することを表し、MixColumns/InvMixColumns演算とは、暗号化時はMixColumn

s演算、復号時はInvMixColumns演算を実行することを表すものとする。

【０３０３】

本実施形態の暗号化時に用いられる実行鍵は、0サイクル目はwkey0とwkey1、1サイクル目はwkey2、…、9サイクル目はwkey10である。復号時に用いられる実行鍵は、0サイクル目はwkey10とwkey9’、1サイクル目はwkey8’、…、9サイクル目はwkey0である。

【０３０４】

本第６の実施形態がトータルで実行している処理は従来技術と同じであるが、本実施形態ではAESの暗号化処理、復号処理を1つ少ないクロックサイクル数で実行することができる。

【０３０５】

次に、本実施形態において各クロックサイクル内で実行される暗号化処理に必要な処理時間について述べる。図４３は、第６の実施形態において各クロックサイクル内で実行される処理に必要な処理時間を従来技術のものと比較して示した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第６の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図４３に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。

【０３０６】

本実施形態では、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行う０サイクル目の処理に必要な処理時間は、AddRoundKey演算、SubBytes演算、ShiftRows演算、MixColumns演算を行う１～８サイクル目の処理に必要な処理時間や、AddRoundKey演算、SubBytes演算、ShiftRows演算を行う９サイクル目の処理に必要な処理時間よりも長い。図４３は復号処理にも対応した図となっており、復号処理に関してもまったく同様のことがいえる。したがって、本第６の実施形態の処理に必要な処理時間の最大値を従来技術のものと比較すると、本第６の実施形態はAddRoundKey演算1回分だけ必要な処理時間が余分にかかる。しかし、AddRoundKey演算1回分の処理時間は、1サイクル内の処理に必要な処理時間全体から見れば非常に小さい。１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、従来技術に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態も多くのケースで実施可能であると想定される。

【０３０７】

ここまでで説明してきた本第６の実施形態の特徴についてまとめる。

【０３０８】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、10サイクル目と0サイクル目に実行される処理に必要な処理時間を合わせても、１～９サイクル目に実行される処理に必要な処理時間に及ばないというように、1サイクル内で実行される処理に必要な処理時間にばらつきがあった。

【０３０９】

一方、本第６の実施形態では1サイクル内で実行される処理に必要な処理時間を均等にするよう暗号化処理、復号処理の処理の区切りを変更した。

【０３１０】

本第６の実施形態は、1サイクル内で実行される処理に必要な処理時間の最大値をわずかに増やすため、従来技術が実施可能な条件下で必ずしも本第６の実施形態が実施可能であるとは限らない。しかし、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理および復号処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０３１１】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。

【０３１２】

図４４は本実施形態のAES処理回路のブロック図を示したものである。図４４において、241はAESの処理を実行するAES処理回路である。242は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。243は鍵拡張部242より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。244はAES処理回路241の外部からの制御信号を受け、鍵拡張部242および暗号化・復号処理部243の動作を制御するための信号を生成し、かつAES処理回路241の外部に対して動作完了を通知するための信号を生成する制御部である。

【０３１３】

なお、同図において第１の実施形態および第２の実施形態で説明した構成要素および信号線と同一のものに関しては、同じであるものとし、その説明を省略する。

【０３１４】

次に、暗号化・復号処理部243について説明する。図４５は暗号化・復号処理部243のブロック図を示したものである。同図において、245は選択信号170、選択信号175および暗号化・復号処理選択信号153による制御を受けながら実行鍵Ａ（162）および実行鍵Ｂ（163）を用いて1サイクル分の暗号化処理もしくは復号処理を行うラウンド処理部である。

【０３１５】

上記構成において、暗号化・復号処理部243のセレクタ109は、選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。

【０３１６】

なお、同図において第１実施形態および第２の実施形態で説明した構成要素および信号線と同一のものに関しては、同様であるのでその説明は省略する。

【０３１７】

次に、ラウンド処理部245について、図４６のブロック図を参照して説明する。同図において、MixColumns/InvMixColumns演算部224には入力信号165および暗号化・復号選択信号153が入力され、セレクタ137にはMixColumns/InvMixColumns演算部224の出力、入力信号165および選択信号175が入力される。AddRoundKey演算部110にはセレクタ137の出力および実行鍵Ａ（162）が入力される。SubBytes/InvSubBytes演算部222にはAddRoundKey演算部110の出力が入力される。ShiftRows/InvShiftRows演算部223にはSubBytes/InvSubBytes演算部222の出力が入力される。AddRoundKey演算部114にはShiftRows/InvShiftRows演算部223の出力および実行鍵Ｂ（163）が入力される。セレクタ115にはShiftRows/InvShiftRows演算部223の出力、AddRoundKey演算部114および選択信号170が入力される。セレクタ115の出力はラウンド処理部245の出力信号168に接続されている。なお、同図において、第１の実施形態、第４の実施形態および第５の実施形態で説明した構成要素および信号線と同一のものに関しては説明を省略した。

【０３１８】

上記構成において、セレクタ137は選択信号175がNegateされている時はMixColumns/InvMixColumns演算部224の出力を、Assertされている時は入力信号165を選択する。セレクタ115は選択信号170がNegateされている時はShiftRows/InvShiftRows演算部223の出力を、Assertされている時はAddRoundKey演算部114の出力を選択する。

【０３１９】

次に、上記構成における暗号化処理時の動作を図２７のタイミングチャートを用いて説明する。なお、同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図４４～図４６で使用されている信号線のナンバと一対一で対応している。

【０３２０】

図２７のタイミングチャートに示される暗号化処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２

つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の暗号化処理期間（T17～T27）、そして４つ目は2ブロック目の暗号化処理期間（T27以降）である。

【０３２１】

パラメータ設定期間の役割、開始条件、終了条件は第３の実施形態と同様である。また、鍵準備期間はT06～T17までの期間である、開始条件、終了条件および各回路の動作も第３の実施形態と同様であるためその説明は省略する。

【０３２２】

制御部244は選択信号175を暗号化処理の終了時にAssertし、暗号化処理の１サイクル目(T18,T28)にNegateする。そして、選択信号170を暗号化処理の最終サイクル（T16）でAssertし、暗号化処理の終了時（T17）にNegateする。さらに、選択信号171を暗号化処理の１サイクル目にAssertし、暗号化処理の終了時にNegateする。

【０３２３】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ115は選択信号170がNegateされている時はShiftRows/InvShiftRows演算部223の出力、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。また、セレクタ137は選択信号175がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時は入力信号165を選択し出力する。また、SubBytes/InvSubBytes演算部222、ShiftRows/InvShiftRows演算部223、およびMixColumns/InvMixColumns演算部224は、暗号化・復号処理選択信号153がNegateされている時はそれぞれSubBytes演算、ShiftRows演算部、MixColumns演算を行い、暗号化・復号処理選択信号153がAssertされている時はそれぞれInvSubBytes演算、InvShiftRows演算部、InvMixColumns演算を行う。

【０３２４】

したがって、ラウンド処理部245は0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、SubBytes演算、ShiftRows演算を行う。1サイクル目からは1サイクル時間前の結果に対して、SubBytes演算、ShiftRows演算、MixColumns演算、AddRoundKey演算を行った結果を出力する。また、9サイクル目（T26～T27）ではMixColumns演算、AddRoundKey演算、SubBytes演算、ShiftRows演算、AddRoundKey演算を行った結果を出力する。

【０３２５】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部245は図４２記載の通りに暗号化処理を実行可能である。

【０３２６】

一方、鍵拡張部242は、鍵準備期間の後、実行鍵Ａ（162）からはwkey0、実行鍵Ｂ（163）からはwkey10を出力している。したがって、暗号化処理の開始時（T17）において、ラウンド処理部245に対してwkey0が供給されている。鍵拡張部242は、暗号化・復号処理開始信号158より暗号化処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey0を用いてwkey1を生成し、実行鍵Ａレジスタに保持する。これによりタイミングT18において、ラウンド処理部245にはwkey1が供給される。以下、タイミングT26まで同様にして実行鍵が供給されていく。タイミングT26では実行鍵Ｂ（163）のwkey10もあわせて供給される。タイミングT26においてwkey10を実行鍵Ａレジスタに保持し、実行鍵の供給がすべて完了すると、鍵拡張部242は次なる暗号化処理の開始に備え、共通鍵152として外部より供給されつづけているwkey0を実行鍵Ａレジスタに保持する(T27)。

【０３２７】

上記のように鍵拡張部242が動作すると、ラウンド処理部245は各サイクルにおいて図４２記載の通りに実行鍵を使用することができる。

【０３２８】

本実施形態の暗号化処理期間の動作は以上のようにして行われる。図２７のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された

場合、AES処理回路はピークの性能を発揮する。しかし、基本的には暗号化処理の間隔は任意の長さとすればよい。

【０３２９】

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０３３０】

続いて、本第６の実施形態の復号処理の動作について述べる。図４７は本第６の実施形態の復号処理のタイミングチャートを示したものである。図４７において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、・・・、T33のタイミング名を割り当てた。また、同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図４４～図４６で使用されている信号線のナンバと一対一で対応している。

【０３３１】

図４７のタイミングチャートに示される復号処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T17）である。３つ目は、1ブロック目の復号処理期間（T17～T27）、そして。４つ目は2ブロック目の復号処理期間（T27以降）である。

【０３３２】

パラメータ設定期間の役割、開始条件、終了条件は本実施形態の暗号化処理時と同様である。ただし、復号処理時は暗号化・復号処理選択信号153はAssertされる。鍵準備期間はT06～T17までであり、開始条件および終了条件は本実施形態の暗号化処理時と同様である。各回路の動作も本実施形態の暗号化処理時とほぼ同様である。ただし、タイミングT16において、実行鍵Ｂ（163）からはwkey10が出力される。また、鍵準備期間の終了時（T17）に制御部244は選択信号175をAssertする。

【０３３３】

1ブロック目の復号処理期間はT17からT27までの期間であり、開始条件および終了条件は本実施形態の暗号化処理時と同様である。各回路の動作もほぼ同様である。

【０３３４】

制御部244は選択信号170を復号処理の最終サイクル(T26)にAssertし、復号処理の１サイクル目(T18,T28)にNegateする。そして、選択信号175を復号処理の終了時（T17）にAssertし、復号処理の終了時（T17）にNegateする。さらに、選択信号171を復号処理の１サイクル目にAssertし、復号処理の終了時にNegateする。

【０３３５】

回路構成を説明する際に述べたとおり、セレクタ109は選択信号171がNegateされている時は入力信号150、Assertされている時はデータ保持部108の出力を選択する。そして、セレクタ137は選択信号175がNegateされている時はMixColumns/InvMixColumns演算部224の出力、Assertされている時は入力信号165を選択し出力する。また、セレクタ115は選択信号170がNegateされている時はShiftRows/InvShiftRows演算部223、Assertされている時はAddRoundKey演算部114の出力を選択し出力する。

【０３３６】

したがって、ラウンド処理部245は、0サイクル目（T17～T18）では入力信号150に対して、AddRoundKey演算、InvShiftRows演算、InvSubBytes演算を行う。1サイクル目からは1サイクル前の結果に対して、AddRoundKey演算、InvMixColumns演算、InvShiftRows演算、InvSubBytes演算を行った結果を出力する。また、9サイクル目（T26～T27）ではAddRoundKey演算、InvMixColumns演算、InvShiftRows演算、InvSubBytes演算、AddRoundKey演算を行った結果を出力する。

【０３３７】

選択信号171、選択信号170、選択信号175を先述のようにコントロールすることでラウンド処理部245は図４２に示した通りに復号処理を実行可能である。

【０３３８】

一方、鍵拡張部242は、鍵準備期間の後、実行鍵Ａ（162）からはwkey10、実行鍵Ｂ（163）からはwkey0を出力している。したがって、復号処理の開始時（T17）において、ラウンド処理部245に対してwkey10が供給されている。鍵拡張部242は、暗号化・復号処理開始信号158より復号処理の開始を検知すると（T17）、実行鍵Ａレジスタに保持されているwkey10’を用いてwkey9’を生成し、実行鍵Ａレジスタに保持する。これによりタイミングT18において、ラウンド処理部245にはwkey9’が供給される。以下同様にして、T19ではwkey9’、T20ではwkey8’、…、T26ではwkey1’が供給される。なお、最終サイクルの処理で必要となるwkey0について実行鍵Ｂ（163）より供給され続けている。

【０３３９】

T26において実行鍵の供給がすべて完了すると、鍵拡張部242は次なる復号処理の開始に備え、次サイクル(T27)にて鍵拡張部242の内部レジスタに保持されているwkey10を用いてwkey9’を生成し、実行鍵Ａレジスタに保持する(T27)。

【０３４０】

本第６の実施形態の復号処理期間の動作は以上のようにして行われる。図４７のタイミングチャートでは1ブロック目の復号処理の終了後、2ブロック目の復号処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの復号処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には復号処理の間隔は任意の長さとすればよい。

【０３４１】

あらかじめ決められたブロック数の復号処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０３４２】

本第６の実施形態は以上のようにして実施可能である。本第６の実施形態は１サイクル内で実行しなければならない処理の処理時間の最大値をわずかに増やすものの、１サイクル内で実行しなければならない処理の処理時間の最大値は1サイクル時間から余裕をもって設定されていることが多いため、大多数のケースでは問題とはならない。そのため、多くのケースでAESの暗号化処理に要するクロックサイクル数を1サイクル削減することができ、これにより約10%程度の処理速度の向上が得られる。

【０３４３】

以上説明した第６の実施形態はあくまで本発明の一例に過ぎず、本発明の効果は上記実施形態に限ったことではない。

【０３４４】

＜第７の実施形態＞

上記第１乃至第６の実施形態において、各クロックサイクル内で実行される処理の処理時間の最大値が1サイクル時間の半分以下の場合、２クロックサイクルかけて行っていた処理を、1クロックサイクル内で実行するように実装し、高速化することが考えられる。そこで本第７の実施形態では、第１の実施形態を例にして、上記高速化手法の実現例を説明する。

【０３４５】

本第７の実施形態における暗号処理回路の暗号化に係る構成は、第１のラウンド処理部と、第２のラウンド処理部と、データ保持部を有する。第１のラウンド処理部は、第１のAddRoundKey演算部、第１のShiftRows演算部、第１のSubBytes演算部、第１のMixColumns演算部、第２のAddRoundKey演算部から構成される。また、第２のラウンド処理部は、第３のAddRoundKey演算部、第２のShiftRows演算部、第２のSubBytes演算部、第２のMixColumns演算部から構成される。

【０３４６】

また、第７の実施形態における暗号復号にかかる構成は、第１のラウンド処理部と、第２のラウンド処理部、及び、データ保持部で構成される。ここで、第１のラウンド処理部は、第１のAddRoundKey演算部、第１のInvShiftRows演算部、第１のInvSubBytes演算部、第１のInvMixColumns演算部、第２のAddRoundKey演算部から構成される。また、第２のラ

ウンド処理部は、第３のAddRoundKey演算部、第２のInvShiftRows演算部、第２のInvSubBytes演算部、第２のInvMixColumns演算部から構成される。

【０３４７】

上記暗号化、復号における構成は以下の説明から明らかにする。

【０３４８】

図４８は第７の実施形態における各クロックサイクル内で実行される暗号化処理の処理内容を従来技術のものと比較して示したものである。

【０３４９】

同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。また、実行鍵wkeyi（iはラウンド数を示す）はFIPS197記載のRound Keyのことである。

【０３５０】

本第７の実施形態は、０サイクル目から３サイクル目では第１のAddRoundKey演算、第１のSubBytes演算、第１のShiftRows演算、第１のMixColumns演算、第２のAddRoundKey演算、第２のSubBytes演算、第２のShiftRows演算、第２のMixColumns演算を実行する。そして、４サイクル目では、第１のAddRoundKey演算、第１のSubBytes演算、第１のShiftRows演算、第１のMixColumns演算、第２のAddRoundKey演算、第２のShiftRows演算、第２のSubBytes演算、第３のAddRoundKey演算を実行する。

【０３５１】

実行鍵は0サイクル目ではwkey0およびwkey1、１サイクル目ではwkey2およびwkey3、…、４サイクル目ではwkey8、wkey9およびwkey10が用いられる。

【０３５２】

本第７の実施形態は従来技術とトータルで実行している処理は同じであるが、本第７の実施形態ではAESの暗号化処理を1つ少ないクロックサイクル数で実行することができる。

【０３５３】

次に、本第７の実施形態において各クロックサイクル内で実行される暗号化処理に必要な処理時間について述べる。図４９は、第７の実施形態において各クロックサイクル内で実行される暗号化処理に必要な処理時間を従来技術のものと比較して示した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第７の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図４９に示すように、各サブブロック演算の処理時間は、SubBytes演算がもっとも長く、次いでMixColumns演算、AddRoundKey演算、ShiftRows演算である。

【０３５４】

本第７の実施形態では、第１のAddRoundKey演算、第１のSubBytes演算、第１のShiftRows演算、第１のMixColumns演算、第２のAddRoundKey演算、第２のSubBytes演算、第２のShiftRows演算、第２のMixColumns演算を行う０～３サイクル目の処理に必要な処理時間は、第１のAddRoundKey演算、第１のSubBytes演算、第１のShiftRows演算、第１のMixColumns演算、第２のAddRoundKey演算、第２のShiftRows演算、第２のSubBytes演算、第３のAddRoundKey演算を行う４サイクル目の処理に必要な処理時間よりも長い。したがって、本第７の実施形態において1サイクル内で実行される処理に必要な処理時間の最大値を従来技術のものと比較すると、両者は等しい。従来技術において1サイクル内で実行される処理に必要な処理時間の最大値が1サイクル時間を下回っていれば、本第７の実施形態もまた実施可能である。

【０３５５】

本発明はAESの復号処理についても同様に適用可能である。

【０３５６】

図５０は第７の実施形態において各クロックサイクル内で実行される復号処理の処理内容を従来例と比較して示したものである。同図において、サイクル数はAESの処理のスタートを0として、そこから経過したクロックサイクル数のことである。

【０３５７】

本第７の実施形態は、0サイクル目では第１のAddRoundKey演算、第１のInvShiftRows演算、第１のInvSubBytes演算、第２のAddRoundKey演算、第１のInvMixColumns演算、第２のInvShiftRows演算、第２のInvSubBytes演算、第３のAddRoundKey演算を行う。そして、１サイクル～４サイクル目では第１のInvMixColumns演算、第１のInvShiftRows演算、第１のInvSubBytes演算、第１のAddRoundKey演算、第２のInvMixColumns演算、第２のInvShiftRows演算、第２のInvSubBytes演算、第２のAddRoundKey演算を実行する。実行鍵は0サイクル目ではwkey10、wkey9およびwkey8、1サイクル目ではwkey7およびwkey6、２サイクル目ではwkey5およびwkey4、…、４サイクル目ではwkey1およびwkey0が用いられる。

【０３５８】

本第７の実施形態は従来技術とトータルで実行している処理は同じであるが、本第７の実施形態ではAESの復号処理を1つ少ないクロックサイクル数で実行することができる。

【０３５９】

次に、本第７の実施形態において各クロックサイクル内で実行される復号処理に必要な処理時間について述べる。図５１は、第７の実施形態において各クロックサイクル内で実行される復号処理に必要な処理時間を従来技術のものと比較して示した図である。縦軸は時間を表しており、棒グラフが長いほど処理時間が長いことを意味する。本第７の実施形態を実現するためには、必要な処理時間の最大値が1サイクル時間を下回っている必要がある。図５１に示すように、各サブブロック演算の処理時間は、InvSubBytes演算がもっとも長く、次いでInvMixColumns演算、AddRoundKey演算、InvShiftRows演算である。

【０３６０】

本第７の実施形態では、第１のInvMixColumns演算、第１のInvShiftRows演算、第１のInvSubBytes演算、第１のAddRoundKey演算、第２のInvMixColumns演算、第２のInvShiftRows演算、第２のInvSubBytes演算、第２のAddRoundKey演算を行う１～４サイクル目の処理に必要な処理時間は、第１のAddRoundKey演算、第１のInvShiftRows演算、第１のInvSubBytes演算、第２のAddRoundKey演算、第１のInvMixColumns演算、第２のInvShiftRows演算、第２のInvSubBytes演算、第３のAddRoundKey演算を行う０サイクル目の処理に必要な処理時間よりも長い。したがって、本第７の実施形態において1サイクル内で実行される処理に必要な処理時間の最大値を従来技術のものと比較すると、両者は等しい。従来技術において1サイクル内で実行される処理に必要な処理時間の最大値が1サイクル時間を下回っていれば、本実施形態もまた実施可能である。

【０３６１】

ここまでで説明してきた本実施形態の特徴についてまとめる。

【０３６２】

従来の一般的な実装方法では、規格にて定義されるラウンド処理を処理の区切りとして、暗号化処理、復号処理を各クロックサイクルごとへ分割していた。そのため、1サイクルあたりの処理に必要な処理時間にばらつきがあった。また、第１の実施形態で示したように処理に要するサイクル数が１１と奇数であるため、2サイクル分の処理を1サイクルで行おうとした場合、1サイクル分の処理が半端になってしまい、結果として6サイクルかけて処理を行うこととなる。

【０３６３】

一方、本発明では第１の実施形態で示したように1サイクルあたりの処理に必要な処理時間を均等にするよう暗号化処理、復号処理をクロックサイクルごとへ分割した結果、処理に要するサイクル数が10サイクルとなった。したがって、2サイクル分の処理を1サイクルで行う場合にも端数が出ない。本第７の実施形態のように2サイクル分の処理を1サイクルで行った場合、1サイクルの削減効果は、約20%程度の処理速度の向上をもたらす。

【０３６４】

次に、上記AESの暗号化処理、復号処理を実現するAES処理回路の回路構成について述べる。

【０３６５】

図５２は、本第７の実施形態のAES処理回路のブロック図を示したものである。

【０３６６】
図５２において、401はAESの処理を実行するAES処理回路である。402は共通鍵からAESの暗号化処理、復号処理に必要となる実行鍵を生成し、出力する鍵拡張部である。403は鍵拡張部402より供給される実行鍵を使って128ビットの平文データの暗号化処理または128ビットの暗号文データの復号処理を実行する暗号化・復号処理部である。404はAES処理回路401の外部からの制御信号を受け、鍵拡張部402および暗号化・復号処理部403の動作を制御するための信号を生成し、かつAES処理回路401の外部に対して動作完了を通知するための信号を生成する制御部である。
【０３６７】
同図において、462は鍵拡張部402で生成された実行鍵のうちの一つであるところの実行鍵Ａ１、463は鍵拡張部402で生成された実行鍵のうちの一つであるところの実行鍵Ａ２である。
【０３６８】
なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては同一参照番号を付し、その説明は省略する。
【０３６９】
上記構成において、実行鍵Ａ１（462）は鍵拡張部402から暗号化・復号処理部403に対して入力され、実行鍵Ａ２（463）は鍵拡張部402から暗号化・復号処理部403に対して入力される。
【０３７０】
次に、暗号化・復号処理部403について説明する。図５３は暗号化・復号処理部403のブロック図を示したものである。同図において、405は実行鍵Ａ１（462）を用いて暗号化処理を行うラウンド処理部である。407は選択信号170による制御を受けながら実行鍵Ａ２（463）および実行鍵Ｂ（163）を用いて暗号化処理を行うラウンド処理部である。406は選択信号170による制御を受けながら実行鍵Ａ１（462）および実行鍵Ｂ（163）を用いて復号処理を行うラウンド処理部である。408は実行鍵Ａ２（463）を用いて復号処理を行うラウンド処理部である。
【０３７１】
同図において、475はラウンド処理部407への入力信号、476はラウンド処理部408への入力信号である。なお、同図において第１の実施形態で説明した構成要素および信号線と同一のものに関しては同一参照番号を付し、その説明は省略する。
【０３７２】
図５４（ａ）はラウンド処理部405、図５４（ｂ）はラウンド処理部407のブロック構成図である。
【０３７３】
まず、ラウンド処理部405について同図（ａ）を用いて説明する。図示において、110は入力信号165および実行鍵Ａ１（462）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。111はAddRoundKey演算部110の出力を入力としSubBytes演算を行うところのSubBytes演算部である。112はSubBytes演算部111の出力を入力としShiftRows演算を行うところのShiftRows演算部である。113はShiftRows演算部112の出力を入力とし、MixColumns演算を行うところのMixColumns演算部である。MixColumns演算部113の出力信号はラウンド処理部405の出力となる。
【０３７４】
次に、ラウンド処理部407について図５４（ｂ）を用いて説明する。図示において、110は入力信号475および実行鍵Ａ２（463）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。111はAddRoundKey演算部110の出力を入力としSubBytes演算を行うところのSubBytes演算部である。112はSubBytes演算部111の出力を入力としShiftRows演算を行うところのShiftRows演算部である。113はShiftRows演算部112の出力を入力とし、MixColumns演算を行うところのMixColumns演算部である。114はShiftRows演算部112の出力および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演

算部である。115は選択信号170に応じてMixColumns演算部113の出力、もしくはAddRoundKey演算部114の出力のいずれか一方を選択し、出力するセレクタである。セレクタ115の出力信号はラウンド処理部407の出力となる。

【０３７５】

なお、上述した各演算の名称はFIPS197に記載されるAES処理の各サブブロック演算と同一である。

【０３７６】

上記構成において、セレクタ115は選択信号170がNegateされている時はMixColumns演算部113の出力、Assertされている時はAddRoundKey演算部114の出力を選択し、出力する。

【０３７７】

次に、ラウンド処理部406、ラウンド処理部408について、図５５（ａ），（ｂ）を参照して説明する。同図（ａ）はラウンド処理部406のブロック図である。

【０３７８】

図示において、116は入力信号165を入力としInvMixColumns演算を行うところのInvMixColumns演算部である。121は入力信号165および実行鍵Ｂ（163）を入力とし、AddRoundKey演算を行うところのAddRoundKey演算部である。118は選択信号170に応じて、InvMixColumns演算部116の出力かAddRoundKey演算部121の出力のいずれか一方を選択し、出力するセレクタである。119はセレクタ118の出力を入力としInvShiftRows演算を行うところのInvShiftRows演算部である。120はInvShiftRows演算部119の出力を入力としInvSubBytes演算を行うところのInvSubBytes演算部である。117はInvSubBytes演算部120の出力および実行鍵Ａ１（462）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。AddRoundKey演算部117の出力はラウンド処理部406の出力となる。

【０３７９】

なお、上述した各演算の名称は、FIPS197に記載されるAES処理の各サブブロック演算と同一である。

【０３８０】

上記構成において、セレクタ118は選択信号170がNegateされている時InvMixColumns演算部116の出力、Assertされている時はAddRoundKey演算部121の出力を選択し、出力する。

【０３８１】

次に、ラウンド処理部408について、図５５（ｂ）のブロック図を参照して説明する。

【０３８２】

同図において、116は入力信号476を入力としInvMixColumns演算を行うところのInvMixColumns演算部である。119はInvMixColumns演算部116の出力を入力としInvShiftRows演算を行うところのInvShiftRows演算部である。120はInvShiftRows演算部119の出力を入力としInvSubBytes演算を行うところのInvSubBytes演算部である。117はInvSubBytes演算部120の出力および実行鍵Ａ２（463）を入力としAddRoundKey演算を行うところのAddRoundKey演算部である。AddRoundKey演算部117の出力はラウンド処理部408の出力となる。

【０３８３】

なお、上述した各演算の名称は、FIPS197に記載されるAES処理の各サブブロック演算と同一である。

【０３８４】

次に、上記構成における暗号化処理時の動作を図５６のタイミングチャートを用いて詳細に説明する。

【０３８５】

図５６において、横軸は時間を示しており、クロックの立ち上がりエッジに合わせてT01、T02、…、T33のタイミング名を割り当てた。また、同図左端に縦方向に並ぶ3桁のナンバは信号線を示しており、図５２～図５５で使用されている信号線の参照番号と一対一で対応している。

【０３８６】

図５６のタイミングチャートに示される暗号化処理時の動作は４つに大別される。１つ目は、共通鍵等の各種パラメータを設定するパラメータ設定期間（T01～T06）である。２つ目は、wkey10を生成しレジスタに保持するための鍵準備期間（T06～T12）である。３つ目は、1ブロック目の暗号化処理期間（T12～T17）、そして、４つ目は、2ブロック目の暗号化処理期間（T17～T22）である。

【０３８７】

パラメータ設定では、共通鍵152、暗号化・復号選択信号153の他、必要に応じて鍵長や暗号モードなど暗号化・復号処理に必要な各種パラメータが設定される。パラメータ設定期間はリセット直後からの任意長の期間であり、AES処理回路401の外部より鍵準備開始信号155がAssertされると（T06）、パラメータ設定期間が終了する。

【０３８８】

パラメータ設定期間が終了すると同時に、次の鍵準備期間が開始される。鍵準備期間は、鍵拡張部において事前に実行鍵を生成するための期間である。鍵準備期間は鍵準備開始信号155がAssertされてから（T06）、最後の実行鍵（wkey10）が生成される6サイクル後（T12）までの期間である。

【０３８９】

次に、鍵準備期間における各回路の動作について述べる。鍵拡張部402はパラメータ設定期間中から、共通鍵152より供給されるwkey0を用いてwkey1の生成を行っており、鍵準備開始信号155がAssertされると同時にwkey1が実行鍵Ａ２（463）のレジスタに保持され、出力される。鍵準備開始信号155のAssertにあわせ、制御部404はカウンタ信号161を0から順次カウントアップする。鍵拡張部402はT07において実行鍵Ａ２（463）に保持されているwkey1を用いて鍵拡張を行いwkey2およびwkey3を生成し、それぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力する。そして、次のサイクル(T08)では実行鍵Ａ２（463）より出力されるwkey3を用いてwkey4およびwkey5を生成し、それぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力する。以下、同様にして実行鍵が生成され、タイミングT09ではwkey6およびwkey7、タイミングT10ではwkey8およびwkey9、がそれぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力される。タイミングT11になると、鍵拡張部402は実行鍵Ａ２（463）より出力されるwkey9を用いてwkey10を生成し、実行鍵Ｂ（163）より出力する。以後、wkey10は再び鍵準備が実行されるまで実行鍵Ｂ（163）より出力され続ける。

【０３９０】

鍵準備期間が終了時（T12）、鍵拡張部402は、共通鍵152より供給されるwkey0をを用いてwkey1を生成し、暗号化・復号処理で最初に用いられる実行鍵（wkey0、wkey1）をそれぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力する。実行鍵Ａ１（462）および実行鍵Ａ２（463）の値は、暗号化・復号処理開始信号158がAssertされるまで保持される。そして、制御部404はカウンタ信号161のカウントアップを停止し、カウンタをゼロクリアする。

【０３９１】

また、鍵準備期間の終了に合わせ、制御部404は鍵準備の開始から5サイクル目（T11）において、次サイクル（T12）で鍵準備が終了し、暗号化処理が可能となることを見越し、暗号化・復号処理許可信号157をAssertする。

【０３９２】

AES処理回路401の外部にある入力信号供給部は、タイミングT12で暗号化・復号処理許可信号157のAssertを検知すると、入力信号150として平文データP0をAES処理回路401に供給する。そして、入力信号150に対する暗号化処理を開始せしめるため、暗号化・復号処理開始信号158をAssertする(T12)。なお、このタイミングチャートでは最短のサイクルで暗号化・復号処理開始信号158がAssertされているが、そのタイミングはAES処理回路401の外部で自由に決められる。

【０３９３】

暗号化処理期間は、入力信号150に対して暗号化処理を行う期間である。暗号化処理期間は、暗号化・復号処理開始信号158がAssert（T12）されてから、その5サイクル後（T17

）までの期間である。

【０３９４】

制御部404は暗号化・復号処理開始信号158のAssertを検知すると、次サイクル（T13）で暗号化・復号処理許可信号157、有効出力期間信号159、出力保持制御信号160をNegateする。同時に、カウンタ信号161のカウントアップを開始する。

【０３９５】

鍵拡張部402は、鍵準備期間と同様に実行鍵の生成を行い、実行鍵Ａ１（462）として、タイミングT12ではwkey0、タイミングT13ではwkey2、…、タイミングT16ではwkey8を出力する。また、実行鍵Ａ２（463）としてタイミングT12ではwkey1、タイミングT13ではwkey3、…、タイミングT16ではwkey9を出力する。

【０３９６】

ラウンド処理部405はタイミングT12～T13では選択信号171がNegateされているため、入力信号150に対して、実行鍵Ａ１として出力されているwkey0を用いて各サブブロック演算を行う。タイミングT13～T17では選択信号171がAssertされている。そのため、ラウンド処理部405は、データ保持部108の出力信号に対して、T13～T14ではwkey2、T14～T15ではwkey4、…、T15～T16ではwkey6を用いてサブブロック演算を行う。

【０３９７】

一方、ラウンド処理部407は入力信号475に対して、T12～T13ではwkey1、T13～T14ではwkey3、T14～T15ではwkey5、…、T15～T16ではwkey7を用いてサブブロック演算を行う。

【０３９８】

暗号化処理の最終サイクルになると（T16）、制御部404は選択信号170をAssertする。それを受け、ラウンド処理部407のセレクタ115は、実行鍵Ｂ（163）を用いてAddRoundKey演算を行うAddRoundKey演算部114の出力を選択し、最終サイクルのサブブロック演算を行う。タイミングT16において、ラウンド処理部407の出力信号166は入力信号である平文データP0を暗号化した結果である暗号文データC0を出力しており、その値は1サイクル後（T17）にデータ保持部108よりAES処理回路401の出力として、外部に出力される。同時に、制御部404は暗号化処理が終了し、出力信号151が有効であることをAES処理回路401の外部に対して通知するため、有効出力期間信号159をAssertする(T17)。有効出力期間信号159がAssertされている間、AES処理回路401は出力信号151が有効であることを保証する。

【０３９９】

一方、出力保持制御信号160は、タイミングT17において有効出力期間信号159がAssertされているものの、同じくT17において暗号化・復号処理開始信号158もまたAssertされているため、Negateされたままである。もしタイミングT17において暗号化・復号処理開始信号158がAssertされなかった場合、T17において出力保持制御信号160がAssertされ、データ保持部108の値は暗号文データC0に保持される。

【０４００】

また、鍵拡張部402は暗号化処理が終了するT17において、実行鍵Ａ１（462）よりwkey0、実行鍵Ａ２（463）よりwkey1を出力する。そして、実行鍵Ａ１（462）および実行鍵Ａ２（463）の値は、次なる暗号化・復号処理開始信号156がAssertされるまで保持される。

【０４０１】

さらに、制御部404は暗号化処理の完了（T17）を見越し、完了の1サイクル前（T16）に暗号化・復号処理許可信号157をAssertする。AES処理回路401の外部は、暗号化・復号処理許可信号157がAssertされていると、入力信号150の値を次なる平文データP1とし、2ブロック目の暗号化処理を開始することが可能となる。図５６のタイミングチャートでは、AES処理回路401の外部は、最短のサイクルで次なる暗号化・復号処理開始信号をAssertしている(T17)。2ブロック目の暗号化処理はT17～T22までであり、1ブロック目と同様の動作が行われる。以降、あらかじめ決められたブロック数の暗号化処理の動作が繰り返し行われる。図５６のタイミングチャートでは1ブロック目の暗号化処理の終了後、2ブロック目の暗号化処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの暗号化処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基

本的には暗号化処理の間隔は任意の長さとすればよい。

【０４０２】

あらかじめ決められたブロック数の暗号化処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０４０３】

続いて、本第７の実施形態の復号処理の動作について説明する。

【０４０４】

図５７は本実施形態の復号処理のタイミングチャートを示したものである。同図において横軸は時間を示しており、クロックの立ち上がりごとにT01、T02、…、T33のタイミング名を割り当てた。また、同図左端に縦方向に並ぶ3桁の番号は信号線を示しており、図５２～図５５で使用されている信号線の参照番号と一対一で対応している。

【０４０５】

復号の場合も４つに大別される。すなわち、パラメータ設定（T01～T06）、鍵準備（T06～T12）、1ブロック目の復号処理（T12～T17）、2ブロック目の復号処理（T17以降）である。

【０４０６】

パラメータ設定期間の役割、開始条件、終了条件は本実施形態の暗号化時と同様である。ただし、復号時は暗号化・復号選択信号153がAssertされる必要がある。

【０４０７】

鍵準備期間はT06～T12までであり、開始条件および終了条件は本実施形態の暗号化時と同様である。各回路の動作も暗号化時とほぼ同様である。ただし、鍵準備期間の終了時（T12）において鍵拡張部402は、実行鍵Ｂ（163）に保持されているwkey10を用いて逆順に鍵拡張を行い、復号処理で最初に用いられる実行鍵（wkey9、wkey8）を実行鍵Ａ１（462）、実行鍵Ａ２（463）よりそれぞれ出力する。実行鍵Ａ１（462）および実行鍵Ａ２（463）の値は、暗号化・復号処理開始信号158がAssertされるまで保持される。そして、制御部404はカウンタ信号161のカウントアップを停止し、カウンタをゼロクリアする。

【０４０８】

また、鍵準備期間の終了に合わせ、制御部404はT11において、T12で鍵準備が終了し、復号処理が可能となることを見越し、暗号化・復号処理許可信号157をAssertする。

【０４０９】

AES処理回路401の外部にある入力信号供給部は、T12で暗号化・復号処理許可信号157のAssertを検知すると、入力信号150として暗号文データC0をAES処理回路401に供給する。そして、入力信号150に対する復号処理を開始せしめるため、暗号化・復号処理開始信号158をAssertする(T12)。なお、このタイミングチャートでは最短のサイクルで暗号化・復号処理開始信号158がAssertされているが、そのタイミングはAES処理回路401の外部で自由に決められる。

【０４１０】

復号処理期間は、入力信号150に対して復号処理を行う期間である。復号処理期間は、暗号化・復号処理開始信号158がAssert（T12）されてから、その5サイクル後（T17）までの期間である。

【０４１１】

制御部404は暗号化・復号処理開始信号158のAssertを検知すると、次サイクル（T13）で暗号化・復号処理許可信号157、有効出力期間信号159、出力保持制御信号160をNegateする。同時に、カウンタ信号161のカウントアップを開始する。

【０４１２】

鍵拡張部402はT13において実行鍵Ａ２（463）に保持されているwkey8を用いて鍵拡張を行いwkey7およびwkey6を生成し、それぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力する。そして、次のサイクル(T14)では実行鍵Ａ２（463）より出力されるwkey6を用いてwkey5およびwkey4を生成し、それぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力する。以下、同様にして実行鍵が生成され、T15ではwkey3およびwkey2、T16ではwkey1お

よびwkey0がそれぞれ実行鍵Ａ１（462）、実行鍵Ａ２（463）より出力される。

【０４１３】

復号処理の最初のサイクル（T12）では、制御部404により選択信号171がNegateされている。そのため、ラウンド処理部406には入力信号150の平文データP0が入力される。ラウンド処理部406は、選択信号170がAssertされているため、AddRoundKey演算部121の出力を選択するようセレクタ118を切り替え、1サイクル分の復号処理が行われる。ラウンド処理部406の出力はそのままラウンド処理部408に対して入力され、さらにもう1サイクル分の復号処理が行われる。ラウンド処理部408で出力結果はデータ保持部108に保持される。

【０４１４】

次サイクル（T13）になると、制御部404により選択信号171がAssertされ、データ保持部の出力がラウンド処理部406に対して入力される。ラウンド処理部406は、選択信号170がNegateされているため、InvMixColumns演算部116の出力を選択するようセレクタ118を切り替え、1サイクル分の復号処理が行われる。ラウンド処理部406の出力はそのままラウンド処理部408に対して入力され、さらにもう1サイクル分の復号処理が行われる。以下、T16まで同様にして処理が行われる。なお、ラウンド処理部406は、実行鍵としてT12ではwkey10およびwkey9、T13ではwkey7、T14ではwkey5、T16ではwkey1を用いる。また、ラウンド処理部408は実行鍵T12ではwkey8、T13ではwkey6、T16ではwkey0を用いる。

【０４１５】

T16において、ラウンド処理部408の出力信号167は入力信号である暗号文データC0を復号した結果である平文データP0を出力しており、その値は1サイクル後（T17）にデータ保持部108よりAES処理回路401の出力として、外部に出力される。同時に、制御部404は復号処理が終了し、出力信号151が有効であることをAES処理回路401の外部に対して通知するため、有効出力期間信号159をAssertする(T17)。有効出力期間信号159がAssertされている間、AES処理回路401は出力信号151が有効であることを保証する。

【０４１６】

一方、出力保持制御信号160は、T17において有効出力期間信号159がAssertされているものの、同じくT17において暗号化・復号処理開始信号158もまたAssertされているため、Negateされたままである。もしT17において暗号化・復号処理開始信号158がAssertされなかった場合、T17において出力保持制御信号160がAssertされ、データ保持部108の値は平文データP0に保持される。

【０４１７】

また、鍵拡張部402は復号処理が終了するT17において、実行鍵Ａ１（462）よりwkey9、実行鍵Ａ２（463）よりwkey8を出力する。そして、実行鍵Ａ１（462）、実行鍵Ａ２（463）の値は、次なる暗号化・復号処理開始信号156がAssertされるまで保持される。

【０４１８】

さらに、制御部404は復号処理の完了（T17）を見越し、完了の1サイクル前（T16）に暗号化・復号処理許可信号157をAssertする。AES処理回路401の外部は、暗号化・復号処理許可信号157がAssertされていると、入力信号150の値を次なる暗号文データC1とし、2ブロック目の復号処理を開始することが可能となる。

【０４１９】

2ブロック目の復号処理期間はT17～T22までであり、1ブロック目と同様の動作が行われる。以降、あらかじめ決められたブロック数の復号処理の動作が繰り返し行われる。図５７のタイミングチャートでは1ブロック目の復号処理の終了後、2ブロック目の復号処理が最短の間隔で実行されている。このようなタイミングですべてのブロックの復号処理が実行された場合、AES処理回路はピークの性能を発揮する。しかし、基本的には復号処理の間隔は任意の長さとすればよい。

【０４２０】

あらかじめ決められたブロック数の復号処理がすべて終了し、次に共通鍵等のパラメータが異なるジョブを実行する際には、再びパラメータ設定から開始される。

【０４２１】

本第７の実施形態は以上のようにして実施可能である。第７の実施形態は、１サイクル内で実行しなければならない処理の処理時間の最大値を増やすことなく、AESの暗号化処理、復号処理に要するクロックサイクル数を1サイクル削減しており、これにより約20%程度の処理速度の向上が得られる。

【０４２２】

なお、ここでは第１の実施形態を例にとって説明したが、他の実施形態についても同様のことが実現できることはいうまでもない。

【０４２３】

以上説明した第７の実施形態はあくまで本発明の一例に過ぎず、本発明の効果は上記実施形態に限ったことではない。

【０４２４】

＜第８の実施形態＞

第７の実施形態の一般形として、第１の実施形態におけるNサイクル分の処理を1クロックサイクルで実行することが考えられる。ただしNは２以上の自然数である。本第８の実施形態では、そのような手法を実現する際の回路構成について述べる。

【０４２５】

第1の実施形態におけるNサイクル分の処理を1クロックサイクルで実行する際、処理に要する総サイクル数をNで割り切れる場合と割り切れない場合の2種類に分類することができる。例えば、AES-128では処理に要する総サイクル数が10であるため（図１）、Nの値が２および５の場合は前者に、それ以外は後者に分類される。

【０４２６】

まず、総サイクル数をNで割り切れる場合について述べる。このような場合、第７の実施形態でN=2のケースについて行ったのと同様に、暗号化処理、復号処理それぞれについてラウンド処理部をＮ個（Ｎは２以上の自然数）ずつ実装し、1クロックサイクルごとにすべてのラウンド処理部を使って処理を行えばよい。このとき、処理に要するクロックサイクル数は10/Nとなる。

【０４２７】

第1の実施形態における総サイクル数をNで割り切れる場合の暗号化・復号処理部の回路構成について説明する。図５８は本第８の実施形態の暗号化・復号処理部のブロック図を示したものである。同図において、503は暗号化・復号処理部、550は実行鍵Ａ１、551は実行鍵Ａ２である。ただし実行鍵Ａは、実行鍵Ａ１（550）、実行鍵Ａ２（551）を含め、Ｎ個存在する。なお、第７の実施形態と同一の構成要素および信号線に関しては同一参照番号を付し、その説明は省略する。

【０４２８】

上記構成において、セレクタ109の出力はラウンド処理部405に接続されている。ラウンド処理部405がＮ－１個直列に接続された後、最後に接続されたラウンド処理部405の出力がラウンド処理部407に接続されている。また、セレクタ109の出力はラウンド処理部406にも接続される。また、ラウンド処理部406の出力はラウンド処理部408に接続されており、ラウンド処理部408がＮ－１個直列に接続された後、最後に接続されたラウンド処理部408の出力がセレクタ107に対して接続されている。ラウンド処理部405には最初に接続されたものから順に実行鍵Ａ１（550）、実行鍵Ａ２（551）、以下別々の実行鍵Ａが入力され、ラウンド処理部407にはＮ個目の実行鍵Ａ、および実行鍵Ｂ（163）が入力されている。また、ラウンド処理部406には実行鍵Ａ１（550）および実行鍵Ｂ（163）が入力されている。また、ラウンド処理部408には接続された順に実行鍵Ａ２（551）以下別々の実行鍵Ａが入力されている。なお、図５８において、第７の実施形態と同一の接続関係のものに関しては説明を省略する。

【０４２９】

次に、第1の実施形態のおける総サイクル数をNで割り切れない場合について述べる。このような場合、暗号化処理、復号処理それぞれについてラウンド処理部をＮ個ずつ実装した上で、暗号化処理または復号処理の特定のサイクルにおいて、一部のラウンド処理部を

バイパスするような構成をとる必要がある。例えばＮ＝４の場合、０クロックサイクル目において、図１の第1の実施形態におけるサイクル数０乃至３の処理を行い、1クロックサイクル目において、図１の第1の実施形態におけるサイクル数４乃至７の処理を行い、２クロックサイクル目において、図１の第1の実施形態におけるサイクル数８乃至９の処理を行う。このように、サイクルの総数がＮで割り切れない場合、０クロックサイクル目および１クロックサイクル目では、４つのラウンド処理部をすべて使用するが、2クロックサイクル目では２つのラウンド処理部だけでよい。このとき、処理に要するクロックサイクル数は10/N（小数点以下切り上げ）となる。

【０４３０】

第1の実施形態における総サイクル数がＮで割り切れない場合の回路構成法は多岐に渡る。例えば、図５８で示した各ラウンド処理部の直後にそれぞれのラウンド処理部をバイパスするか否かを選択するためのセレクタを設け、暗号化処理または復号処理の開始からのサイクル数に応じてセレクタを切り替えるといった手法が考えられる。このケースの回路構成に関しては図５８より容易に想像可能なため、ブロック図は省略する。

【０４３１】

本第８の実施形態は以上のようにして実現可能である。本発明の第１の実施形態によれば、AES-128の処理に要する総クロックサイクル数は10、AES-192は12、AES-256は14である。いずれも本実施形態で述べたのと同様、サイクルの総数をＮで割り切れる場合、割り切れない場合に分類し、実現することができる。また、AES-128、AES-192、AES-256すべてを実現する回路構成をとることも可能である。この場合、Ｎ＝１およびＮ＝２としたときは、AES-128、AES-192、AES-256いずれも処理に要する総クロックサイクル数がＮで割り切れるため、本実施形態における総クロックサイクル数をＮで割り切れる場合と同様にして実現可能である。Ｎの値がそれ以外であっても、本実施形態における、第1の実施形態における総サイクル数をNで割り切れない場合、と同様、暗号化・復号処理部に実装されたN個のラウンド処理部のうち、任意のラウンド処理部の出力を暗号化・復号処理部の出力として選択可能な構成とすることで、AES-128、AES-192、AES-256すべてを実現する回路構成が可能である。

【０４３２】

＜第９の実施形態＞

本発明の第１乃至６の実施形態において、規定された1クロックサイクル内に1サイクルの処理が収まらない場合も存在する。そのような場合、ラウンド処理部に新たにデータ保持部を追加し、第１乃至第６の実施形態における1サイクルの処理を、複数クロックサイクルかけて実行するような実装法が考えられる。ここでは具体例として、第１の実施形態において1サイクルで実行している処理を、2クロックサイクルかけて実行する場合の回路構成について説明する。

【０４３３】

図５９は第１の実施形態のラウンド処理部に新たにデータ保持部を追加した例を示している。同図において、605はラウンド処理部、608は暗号化処理の途中結果を保持するためのデータ保持部である。

【０４３４】

上記構成において、データ保持部608にはSubBytes演算部111の出力が入力され、データ保持部608の出力はShiftRows演算部112に入力されている。

【０４３５】

このように暗号化処理部に新たにデータ保持部を1つ追加することで、第１の実施形態における1サイクル分の処理を、2クロックサイクルかけて行うように変更することができる。図５９では、SubBytes演算部111とShiftRows演算部112の間にデータ保持部608を追加しているが、データ保持部は任意の場所に接続すればよい。あるいは、SubBytes演算部111の内部にデータ保持部を設けてもよい。

【０４３６】

また、ここでは第１の実施形態における1サイクル分の処理に、2クロックサイクルをか

ける場合を例にとったが、Nクロックサイクルをかけることもできる。その場合、新たにN-1個のデータ保持部を各演算部間の任意の場所、あるいは各演算部の内部に実装すればよい。

【０４３７】

なお、ここでは第１の実施形態を例にとって説明したが、他の実施形態についても同様のことが実現できることはいうまでもない。

【０４３８】

＜第１０の実施形態＞

本発明の第１乃至９の実施形態では、データ保持部のデータ更新周期を１クロックサイクルとしてきたが、必ずしもそうである必要はない。

【０４３９】

一般にCPUやDMAを動作クロックの周波数は高いことが多く、同じクロックを暗号処理のデータ保持部で用いると、暗号処理に必要な処理時間が確保できず、1クロックサイクルに収まらないことがある。このようなとき、例えば、暗号処理に必要な処理時間が1クロックサイクルの2倍以内であれば、2クロックサイクルに1回データ保持部のデータ更新を行ってもよい。

【０４４０】

このような構成は、データ保持部に対して新たにイネーブル信号を入力することで、簡単に実現可能である。

【０４４１】

図６１（ａ）、（ｂ）のタイミングチャートを用いて、本実施形態を説明する。図６１（ａ）は、クロックサイクルとデータ保持部のデータ更新が同期している場合のタイミングチャートを示している。クロックサイクルの立ち下がりエッジと同期して、データ保持部はそのデータを更新する。

【０４４２】

一方、図６１（ｂ）は、クロックサイクルとデータ保持部のデータ更新が非同期の場合のタイミングチャートを示している。イネーブル信号はデータ保持部に対して入力されており、クロックの１／２の周期でHIGH/LOWを繰り返している。データ保持部はイネーブル信号がHIGHの時のみデータ更新を行うため、２回に１回、クロックの立下りエッジに合わせてデータを更新する。

この場合、2クロックサイクルかけて、1サイクル分の処理が行われることになる。

【０４４３】

本実施形態では、2クロックサイクルをかけて1サイクル分の処理を行う例を説明したが、Nクロックサイクルかけて1サイクル分の処理をしてもよいことは言うまでも無い。

【０４４４】

本発明の第１乃至９の実施形態において、Nクロックサイクルを1サイクルとした構成を取る事もできる。

【０４４５】

以上本発明にかかる実施形態を説明した。各実施形態では、AES-128を例にとって説明したが、AES-192、AES-256についても実現可能である。AES-128の実施形態と異なるものは、鍵拡張部に入力される共通鍵のビット数、鍵拡張部にて生成される実行鍵の数、および各制御信号のAssert/Negateのタイミングである。これらは、各実施形態の説明で述べたものと同様の考え方で、容易に実現可能である。暗号化・復号処理部およびラウンド処理部はAES-128の実施形態で述べたものからの変更を要しない。

【図面の簡単な説明】

【０４４６】

【図１】従来技術と第１の実施形態における各クロックサイクル内で実行される暗号化処理の処理内容を比較するための図である。

【図２】従来技術と第１の実施形態における各クロックサイクル内で実行される暗号化処理に必要な処理時間を比較するための図である。

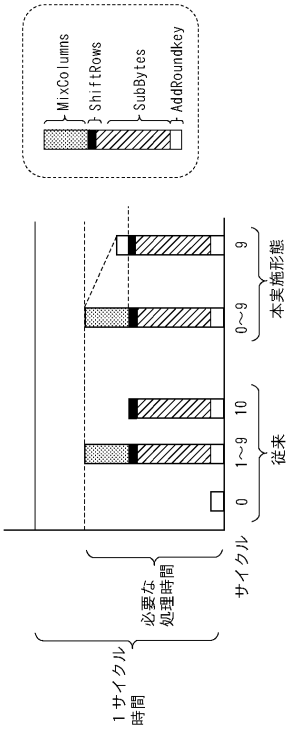
【図３】従来技術と第１の実施形態における各クロックサイクル内で実行されるの復号処理の処理内容を比較するための図である。
【図４】従来技術と第１の実施形態における各クロックサイクル内で実行される復号処理に必要な処理時間を比較するための図である。
【図５】第１の実施形態におけるAES処理回路のブロック図である。
【図６】第１の実施形態における暗号化・復号処理部のブロック図である。
【図７】第１の実施形態における暗号化のラウンド処理部のブロック図である。
【図８】第１の実施形態における復号のラウンド処理部のブロック図である。
【図９】第１の実施形態における暗号化処理時のタイミングチャートである。
【図１０】第１の実施形態における復号処理時のタイミングチャートである。
【図１１】第２の実施形態における各クロックサイクル内で実行される暗号化処理、復号処理の処理内容を示す図である。
【図１２】従来技術と第２の実施形態における各クロックサイクル内で実行される暗号化処理に必要な処理時間を比較するための図である。
【図１３】従来技術と第２の実施形態における各クロックサイクル内で実行される復号処理に必要な処理時間を比較するための図である。
【図１４】第２の実施形態におけるAES処理回路のブロック図である。
【図１５】第２の実施形態における暗号化・復号処理部のブロック図である。
【図１６】第２の実施形態における暗号化のラウンド処理部のブロック図である。
【図１７】第２の実施形態における復号のラウンド処理部のブロック図である。
【図１８】第２の実施形態における暗号化処理時のタイミングチャートである。
【図１９】第２の実施形態における復号処理時のタイミングチャートである。
【図２０】第３の実施形態における各クロックサイクル内で実行される暗号化処理、復号処理の処理内容を示す図である。
【図２１】従来技術と第３の実施形態における各クロックサイクル内で実行される暗号化処理に必要な処理時間を比較するための図である。
【図２２】従来技術と第３の実施形態における各クロックサイクル内で実行される復号処理に必要な処理時間を比較するための図である。
【図２３】第３の実施形態におけるAES処理回路のブロック図である。
【図２４】第３の実施形態における暗号化・復号処理部のブロック図である。
【図２５】第３の実施形態における暗号化のラウンド処理部のブロック図である。
【図２６】第３の実施形態における復号のラウンド処理部のブロック図である。
【図２７】第３の実施形態における暗号化処理時のタイミングチャートである。
【図２８】第３の実施形態における復号処理時のタイミングチャートである。
【図２９】従来技術と第４の実施形態における各クロックサイクル内で実行される暗号化処理の処理内容を比較するための図である。
【図３０】従来技術と第４の実施形態における各クロックサイクル内で実行される復号処理の処理内容を比較するための図である。
【図３１】従来技術と第４の実施形態における各クロックサイクル内で実行される処理に必要な処理時間を比較するための図である。
【図３２】第４の実施形態におけるAES処理回路のブロック図である。
【図３３】第４の実施形態における暗号化・復号処理部のブロック図である。
【図３４】第４の実施形態におけるラウンド処理部のブロック図である。
【図３５】第４の実施形態における復号処理時のタイミングチャートである。
【図３６】第５の実施形態における各クロックサイクル内で実行される暗号化処理、復号処理の処理内容である。
【図３７】従来技術と第５の実施形態における各クロックサイクル内で実行される処理に必要な処理時間の比較である。
【図３８】第５の実施形態におけるAES処理回路のブロック図である。
【図３９】第５の実施形態における暗号化・復号処理部のブロック図である。

【図４０】第５の実施形態におけるラウンド処理部のブロック図である。
【図４１】第５の実施形態における復号処理時のタイミングチャートである。
【図４２】第６の実施形態における各クロックサイクル内で実行される暗号化処理、復号処理の処理内容である。
【図４３】従来技術と第６の実施形態における各クロックサイクル内で実行される処理に必要な処理時間を比較するための図である。
【図４４】第６の実施形態におけるAES処理回路のブロック図である。
【図４５】第６の実施形態における暗号化・復号処理部のブロック図である。
【図４６】第６の実施形態におけるラウンド処理部のブロック図である。
【図４７】第６の実施形態における復号処理時のタイミングチャートである。
【図４８】従来技術と第７の実施形態における各クロックサイクル内で実行される暗号化処理の処理内容を比較するための図である。。
【図４９】従来技術と第７の実施形態における各クロックサイクル内で実行される暗号化処理に必要な処理時間を比較するための図である。
【図５０】従来技術と第７の実施形態における各クロックサイクル内で実行される復号処理の処理内容を比較するための図である。
【図５１】従来技術と第７の実施形態における各クロックサイクル内で実行される復号処理に必要な処理時間を比較するための図である。
【図５２】第７の実施形態におけるAES処理回路のブロック図である。
【図５３】第７の実施形態における暗号化・復号処理部のブロック図である。
【図５４】第７の実施形態における暗号化のラウンド処理部のブロック図である。
【図５５】第７の実施形態における復号のラウンド処理部のブロック図である。
【図５６】第７の実施形態における暗号化処理時のタイミングチャートである。
【図５７】第７の実施形態における復号処理時のタイミングチャートである。
【図５８】第８の実施形態における暗号化・復号処理部のブロック図である。
【図５９】第９の実施形態におけるラウンド処理部のブロック図である。
【図６０】AESのアルゴリズムを示す図である。
【図６１】クロックとデータ保持部のデータ更新タイミングを示す図である。
【図６２】他の実装方法を示す図である。

【図１】

サイクル数	従来		第1の実施形態	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey	・0番目の実行鍵 ($wkey_0$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns	・0番目の実行鍵 ($wkey_0$)
1	• SubBytes • ShiftRows • MixColumns • AddRoundKey	・1番目の実行鍵 ($wkey_1$)	• AddRoundKey • SubBytes • ShiftRows • MixColumns	・1番目の実行鍵 ($wkey_1$)
8	•SubBytes •ShiftRows •MixColumns •AddRoundKey	・8番目の実行鍵 ($wkey_8$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns	・8番目の実行鍵 ($wkey_8$)
9	•SubBytes •ShiftRows •MixColumns •AddRoundKey	・9番目の実行鍵 ($wkey_9$)	•AddRoundKey •SubBytes •ShiftRows •AddRoundKey	・9番目の実行鍵 ($wkey_9$) ・10番目の実行鍵 ($wkey_{10}$)
10	•SubBytes •ShiftRows •AddRoundKey	・10番目の実行鍵 ($wkey_{10}$)		

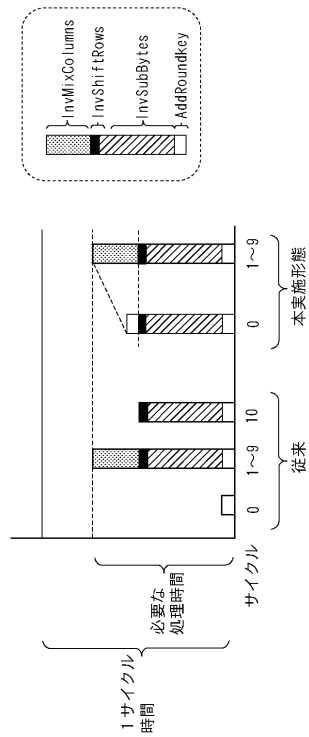
【図２】



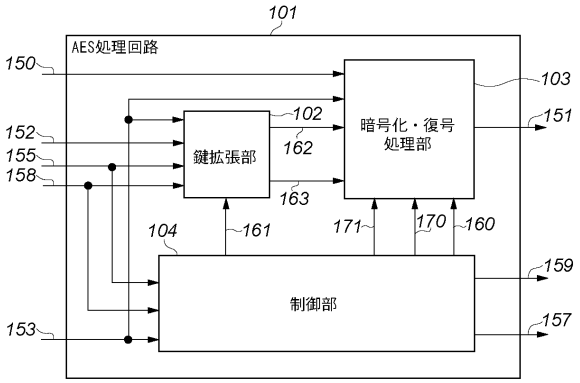
【図３】

サイクル数	従来		第1の実施形態	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey	・10番目の実行鍵 ($wkey_{10}$)	•AddRoundKey •InvShiftRows •InvSubBytes •AddRoundKey	・10番目の実行鍵 ($wkey_{10}$) ・9番目の実行鍵 ($wkey_9$)
1	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	・9番目の実行鍵 ($wkey_9$)	•InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	・8番目の実行鍵 ($wkey_8$)
8	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	・2番目の実行鍵 ($wkey_2$)	•InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	・1番目の実行鍵 ($wkey_1$)
9	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	・1番目の実行鍵 ($wkey_1$)	•InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	・0番目の実行鍵 ($wkey_0$)
10	•InvShiftRows •InvSubBytes •	・0番目の実行鍵 ($wkey_0$)		

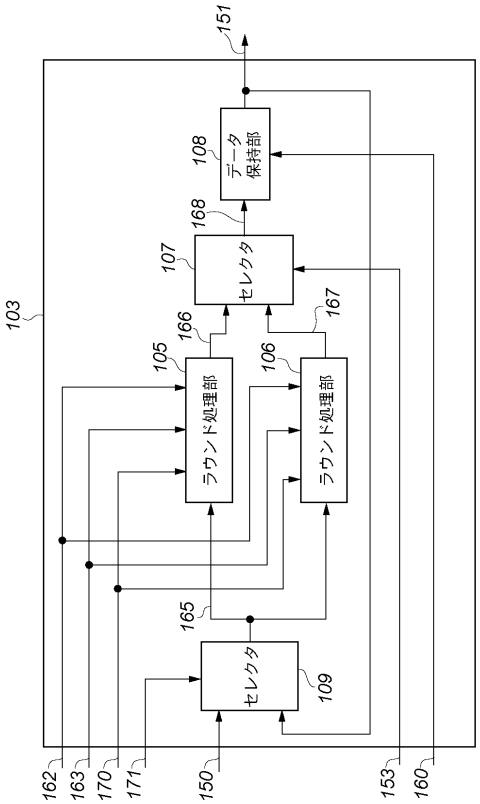
【図４】



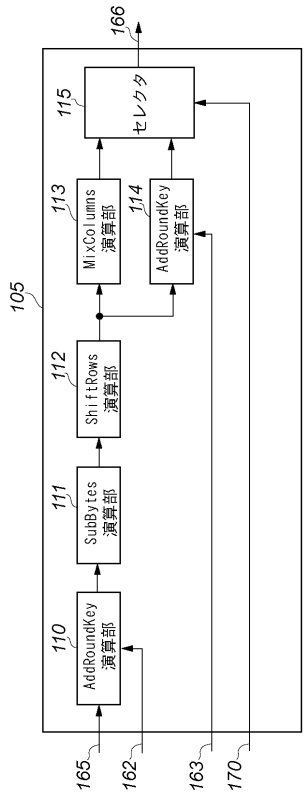
【図５】


101
AES処理回路
150
152
155
158
153
鍵拡張部
102
162
163
暗号化・復号
処理部
103
151
104
161
171
170
160
制御部
159
157

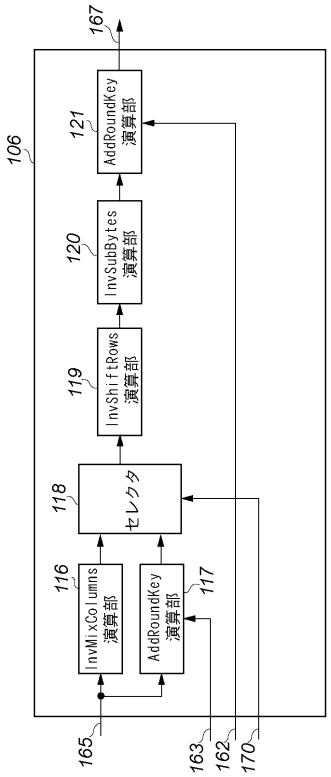
【図６】


151
108
データ
保持部
168
107
セレクタ
167
103
166
105
ラウンド処理部
106
ラウンド処理部
165
セレクタ
109
162
163
170
171
150
153
160

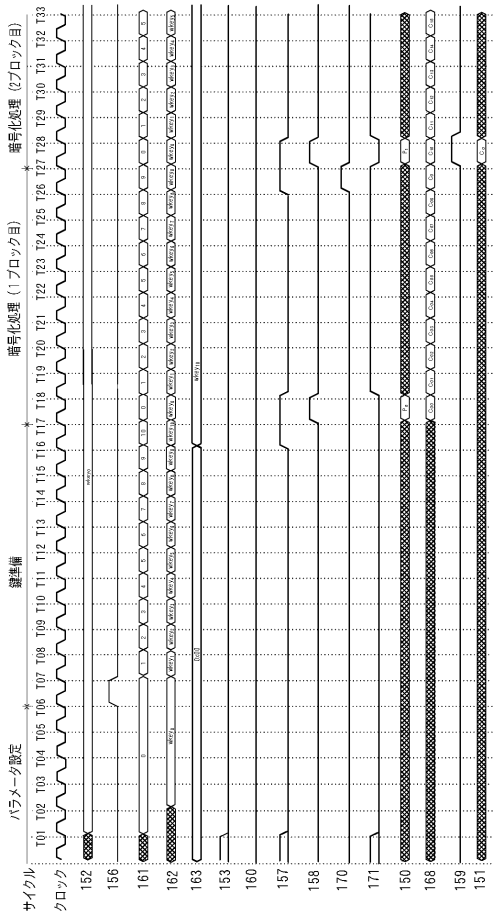
【図７】


166
115
セレクタ
105
113
MixColumns
演算部
114
AddRoundKey
演算部
112
ShiftRows
演算部
111
SubBytes
演算部
110
AddRoundKey
演算部
165
162
163
170

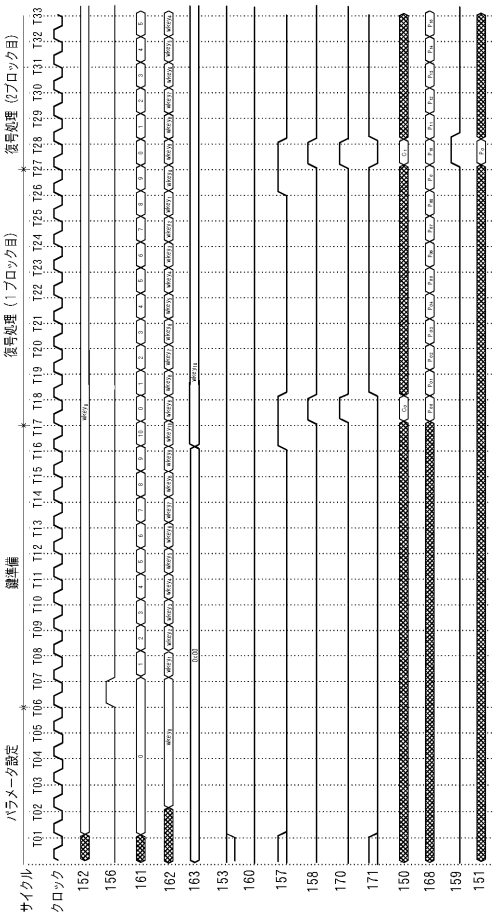
【図８】


167
106
121
AddRoundKey
演算部
120
InvSubBytes
演算部
119
InvShiftRows
演算部
118
セレクタ
116
InvMixColumns
演算部
AddRoundKey
演算部
117
165
163
162
170

【図９】



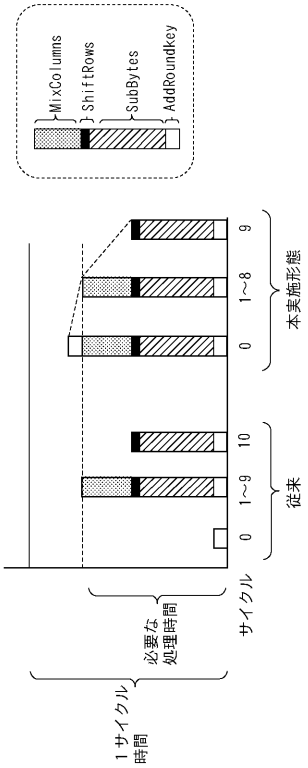
【図１０】



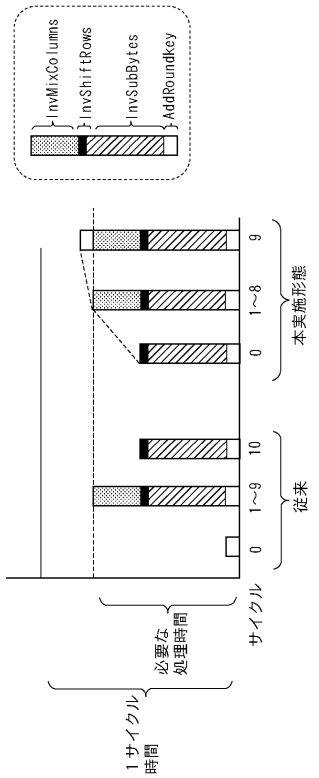
【図１１】

サイクル数	暗号化時の処理		復号時の処理	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	・AddRoundKey ・SubBytes ・ShiftRows ・MixColumns ・AddRoundKey	・0番目の実行鍵 ($wkey_0$) ・1番目の実行鍵 ($wkey_1$)	・AddRoundKey ・InvShiftRows ・InvSubBytes	・10番目の実行鍵 ($wkey_{10}$)
1	・SubBytes ・ShiftRows ・MixColumns ・AddRoundKey	・2番目の実行鍵 ($wkey_2$)	・AddRoundKey ・InvMixColumns ・InvShiftRows ・InvSubBytes	・9番目の実行鍵 ($wkey_9$)
8	・SubBytes ・ShiftRows ・MixColumns ・AddRoundKey	・9番目の実行鍵 ($wkey_9$)	・AddRoundKey ・InvMixColumns ・InvShiftRows ・InvSubBytes	・2番目の実行鍵 ($wkey_2$)
9	・SubBytes ・ShiftRows ・AddRoundKey	・10番目の実行鍵 ($wkey_{10}$)	・AddRoundKey ・InvMixColumns ・InvShiftRows ・InvSubBytes ・AddRoundKey	・1番目の実行鍵 ($wkey_1$) ・0番目の実行鍵 ($wkey_0$)

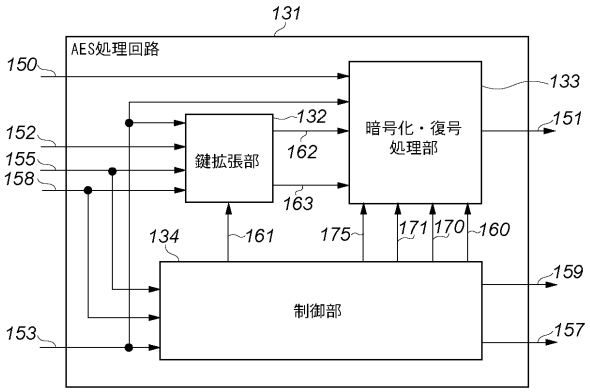
【図１２】



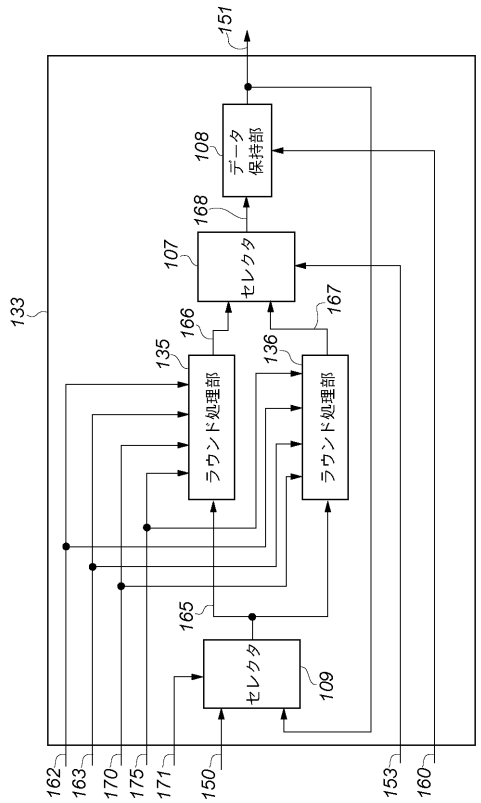
【図１３】



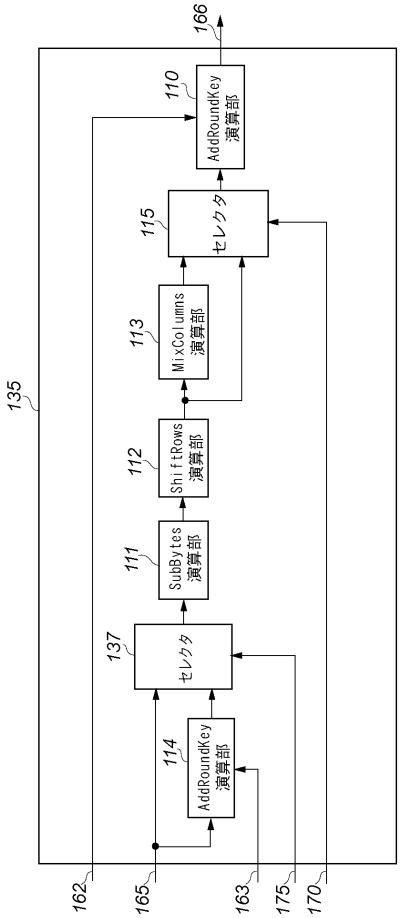
【図１４】



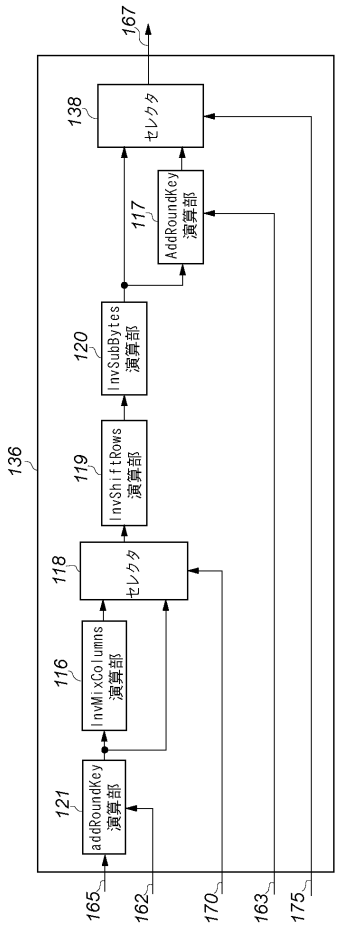
【図１５】



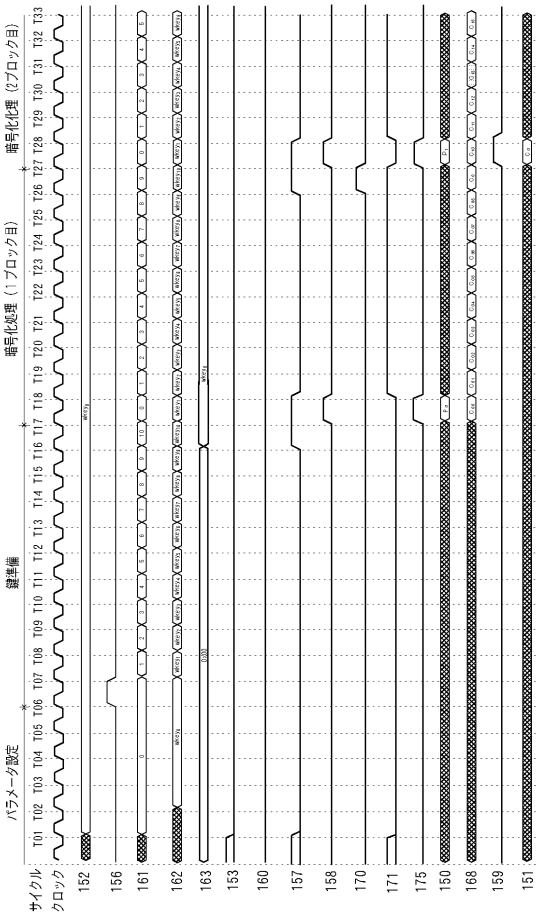
【図１６】



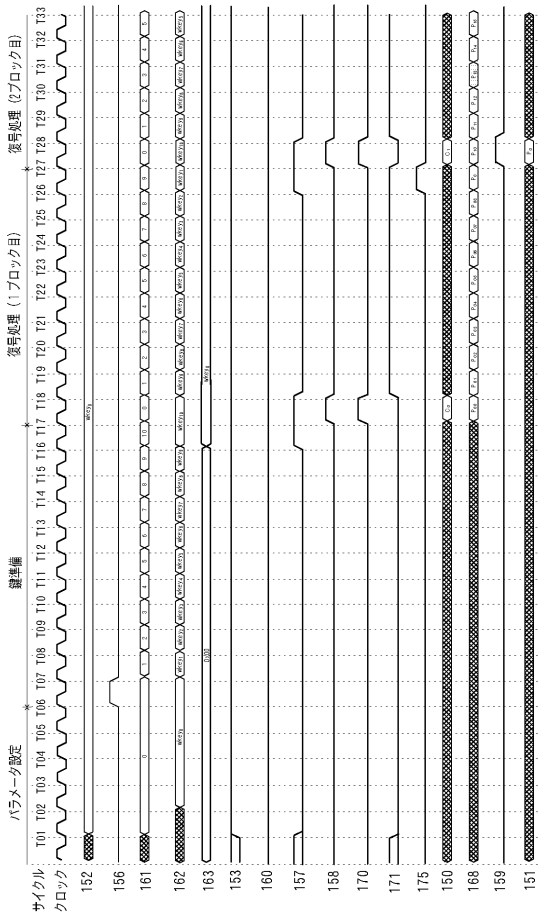
【図１７】



【図１８】



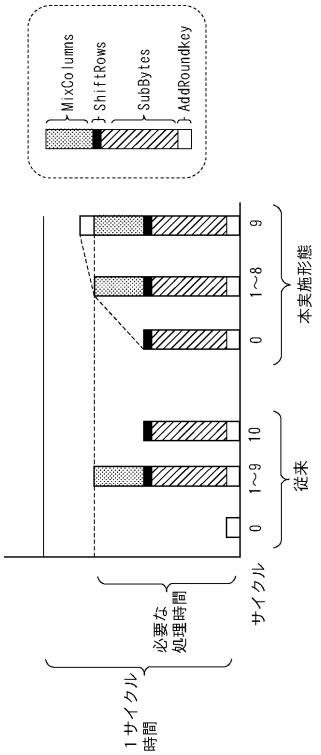
【図１９】



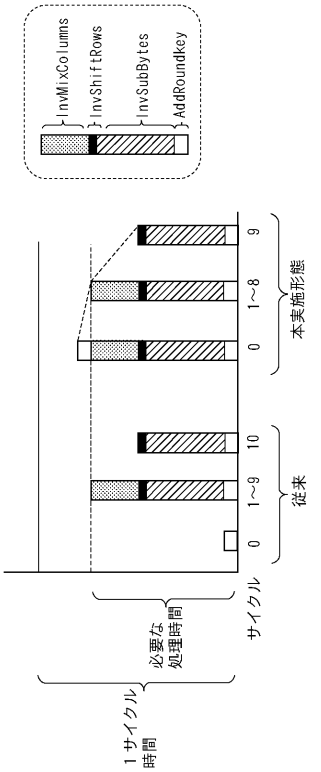
【図２０】

処理開始からのクロックサイクル数	暗号化時の処理		復号時の処理	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey •SubBytes •ShiftRows	•0番目の実行鍵 ($wkey_0$)	•AddRoundKey •InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	•10番目の実行鍵 ($wkey_{10}$) •9番目の実行鍵 ($wkey_9$)
1	•MixColumns •AddRoundKey •SubBytes •ShiftRows	•1番目の実行鍵 ($wkey_1$)	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	•8番目の実行鍵 ($wkey_8$)
8	•MixColumns •AddRoundKey •SubBytes •ShiftRows	•8番目の実行鍵 ($wkey_8$)	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	•1番目の実行鍵 ($wkey_1$)
9	•MixColumns •AddRoundKey •SubBytes •ShiftRows •AddRoundKey	•9番目の実行鍵 ($wkey_9$) •10番目の実行鍵 ($wkey_{10}$)	•InvShiftRows •InvSubBytes •AddRoundKey	•0番目の実行鍵 ($wkey_0$)

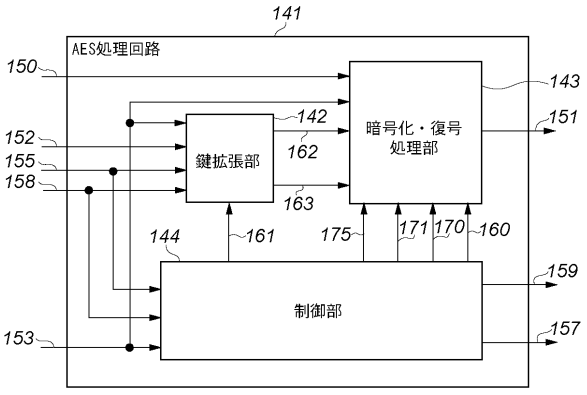
【図２１】



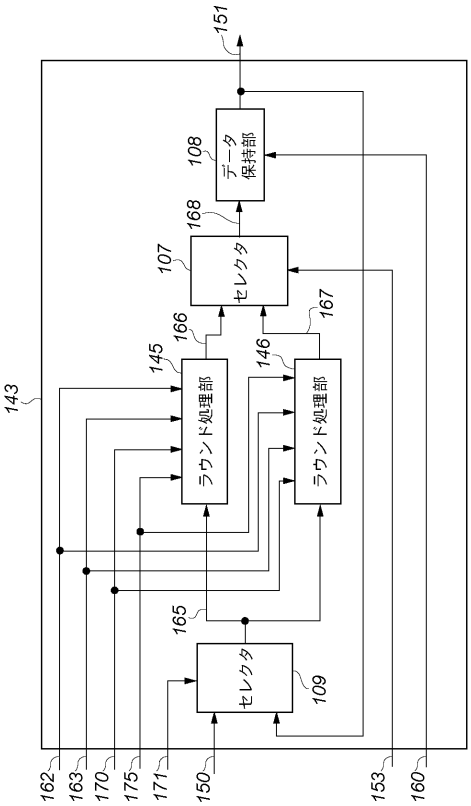
【図２２】



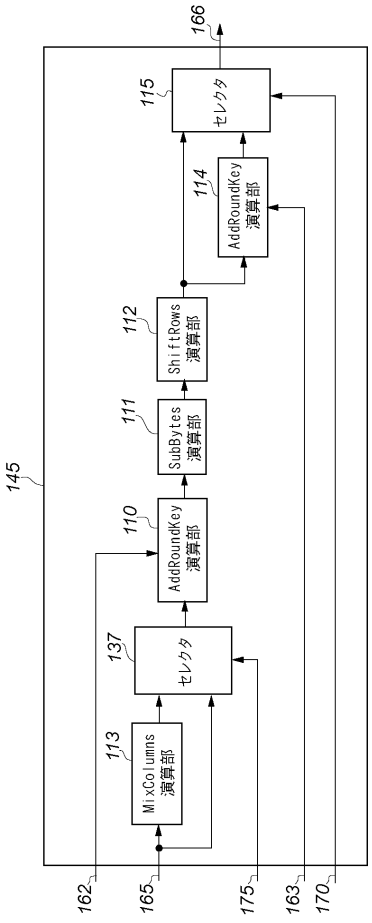
【図２３】



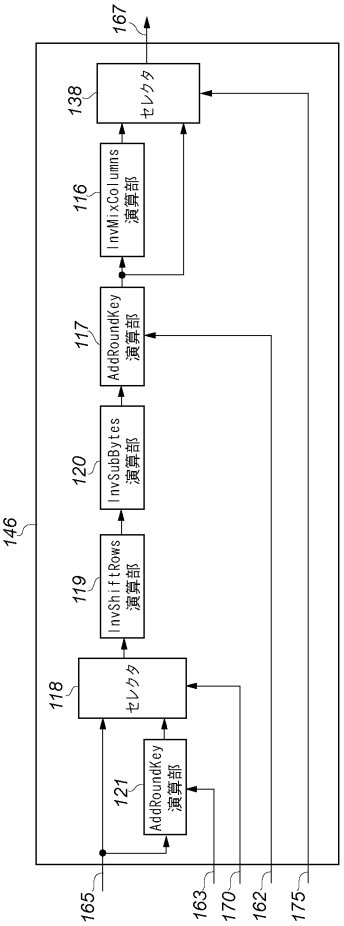
【図２４】



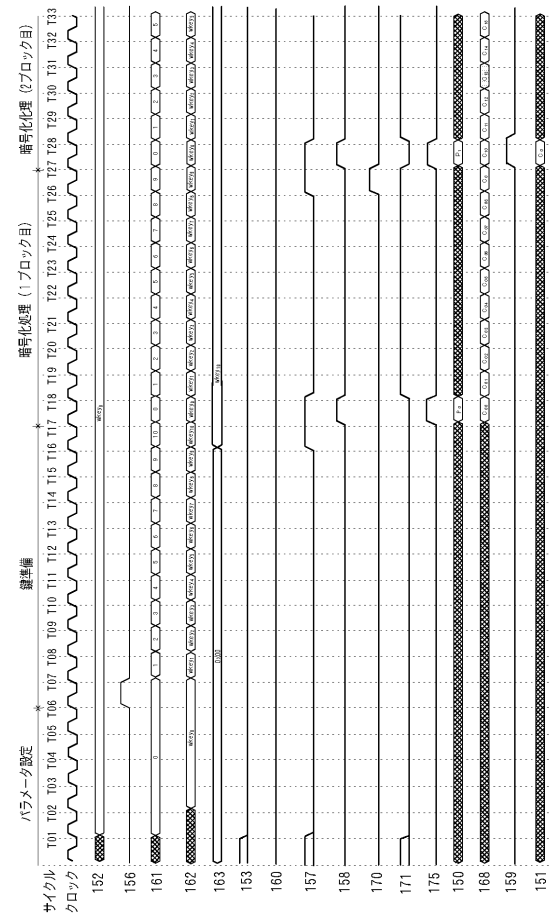
【図２５】



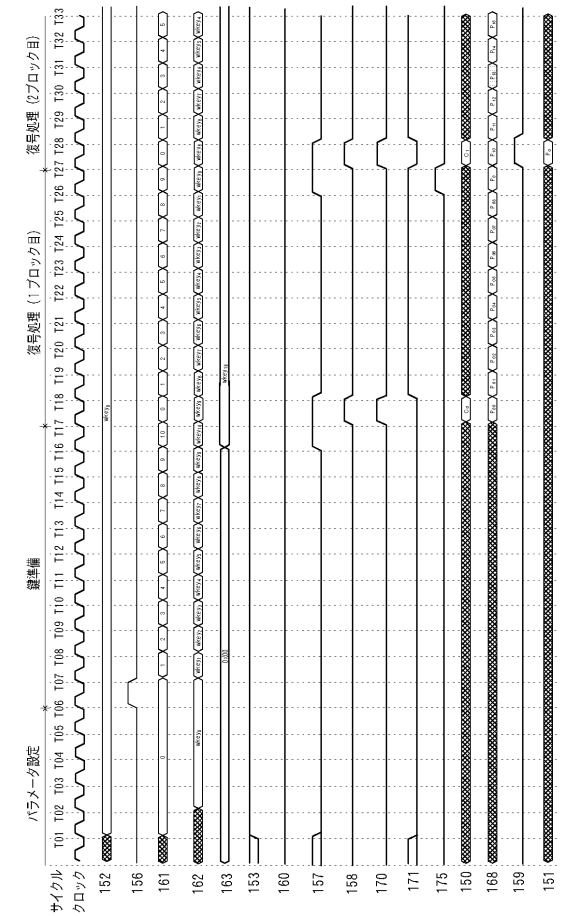
【図２６】



【図２７】



【図２８】



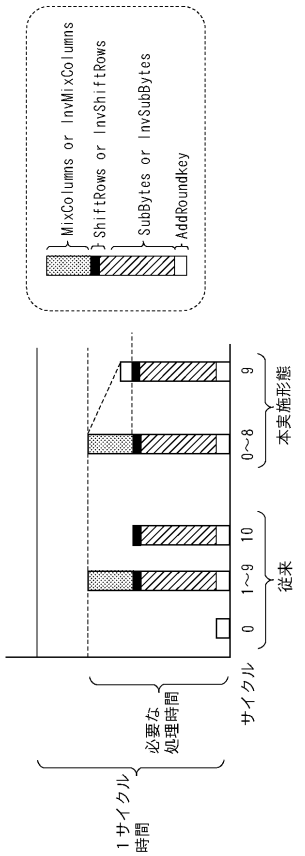
【図２９】

サイクル数	従来		実施形態４	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey	・0番目の実行鍵 ($wkey_0$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns	・0番目の実行鍵 ($wkey_0$)
1	•SubBytes •ShiftRows •MixColumns •AddRoundKey	・1番目の実行鍵 ($wkey_1$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns	・1番目の実行鍵 ($wkey_1$)
8	•SubBytes •ShiftRows •MixColumns •AddRoundKey	・8番目の実行鍵 ($wkey_8$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns	・8番目の実行鍵 ($wkey_8$)
9	•SubBytes •ShiftRows •MixColumns •AddRoundKey	・9番目の実行鍵 ($wkey_9$)	•AddRoundKey •SubBytes •ShiftRows •AddRoundKey	・9番目の実行鍵 ($wkey_9$) ・10番目の実行鍵 ($wkey_{10}$)
10	•SubBytes •ShiftRows •AddRoundKey	・10番目の実行鍵 ($wkey_{10}$)		

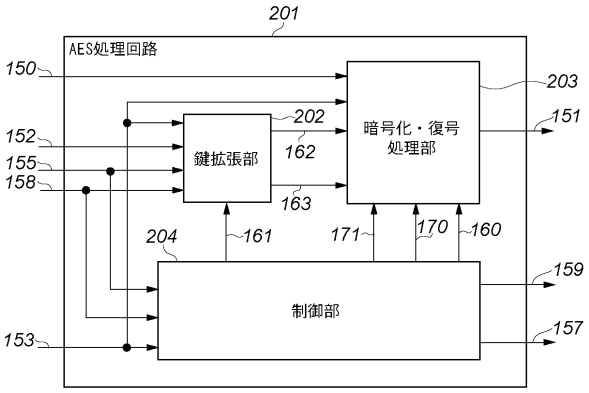
【図３０】

サイクル数	従来		実施形態４	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey	•10番目の実行鍵 ($wkey_{10}$)	•AddRoundKey •InvSubBytes •InvShiftRows •InvMixColumns	•10番目の実行鍵 ($wkey_{10}$)
1	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•9番目の特殊実行鍵 ($wkey_9'$)	•AddRoundKey •InvSubBytes •InvShiftRows •InvMixColumns	•9番目の特殊実行鍵 ($wkey_9'$)
8	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•2番目の特殊実行鍵 ($wkey_2'$)	•AddRoundKey •InvSubBytes •InvShiftRows •InvMixColumns	•2番目の特殊実行鍵 ($wkey_2'$)
9	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•1番目の特殊実行鍵 ($wkey_1'$)	•AddRoundKey •InvSubBytes •InvShiftRows •AddRoundKey	•1番目の特殊実行鍵 ($wkey_1'$) •0番目の実行鍵 ($wkey_0$)
10	•InvSubBytes •InvShiftRows •AddRoundKey	•0番目の実行鍵 ($wkey_0$)		

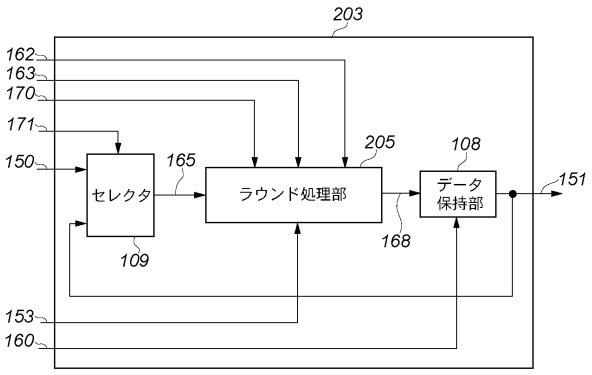
【図３１】



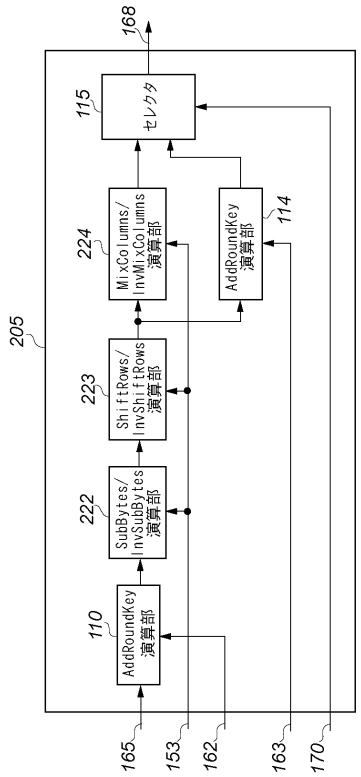
【図３２】



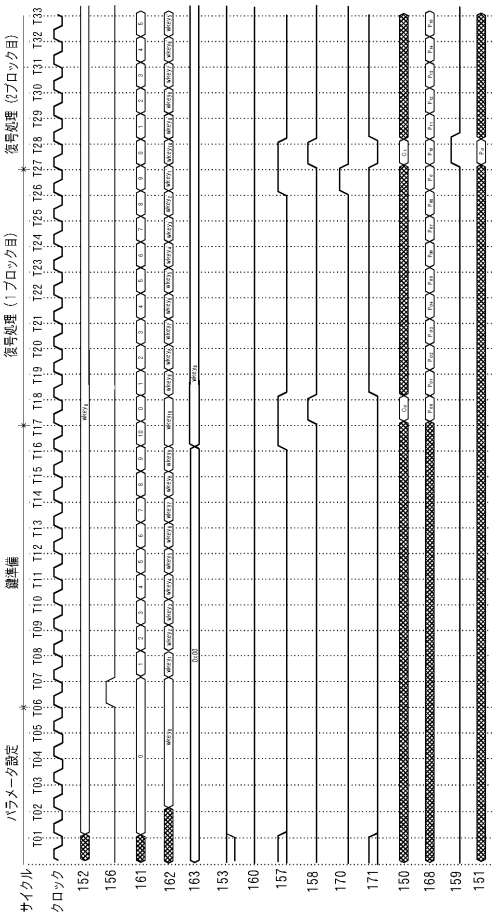
【図３３】



【図３４】



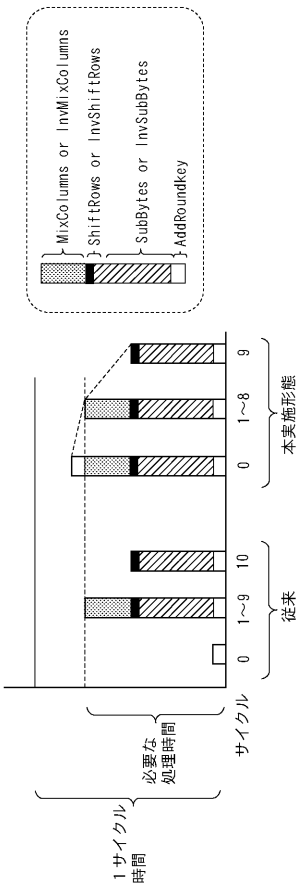
【図３５】



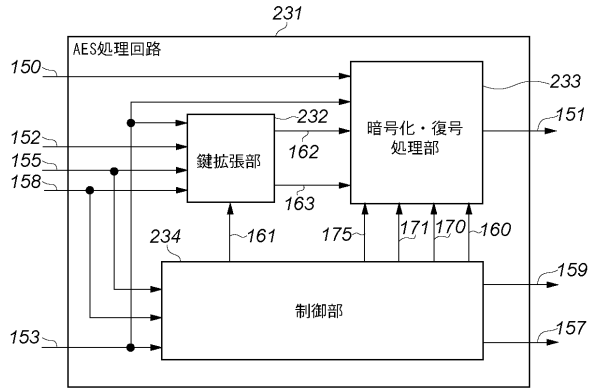
【図３６】

サイクル数	暗号化時の処理		復号時の処理	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey	•0番目の実行鍵 ($wkey_0$) •1番目の実行鍵 ($wkey_1$)	•AddRoundKey •InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•10番目の実行鍵 ($wkey_{10}$) •9番目の特殊実行鍵 ($wkey_9'$)
1	•SubBytes •ShiftRows •MixColumns •AddRoundKey	•2番目の実行鍵 ($wkey_2$)	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•8番目の特殊実行鍵 ($wkey_8'$)
8	•SubBytes •ShiftRows •MixColumns •AddRoundKey	•9番目の実行鍵 ($wkey_9$)	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•1番目の特殊実行鍵 ($wkey_1'$)
9	•SubBytes •ShiftRows •AddRoundKey	•10番目の実行鍵 ($wkey_{10}$)	•InvSubBytes •InvShiftRows •AddRoundKey	•0番目の実行鍵 ($wkey_0$)

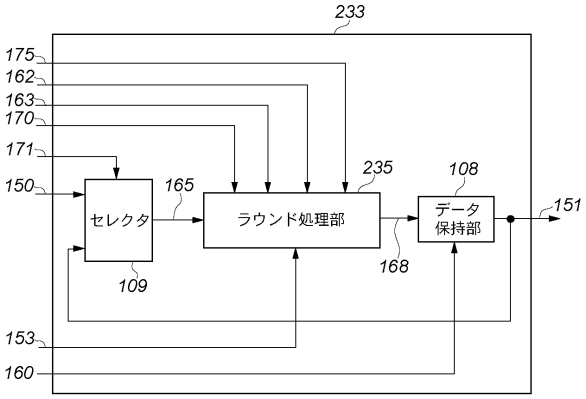
【図３７】



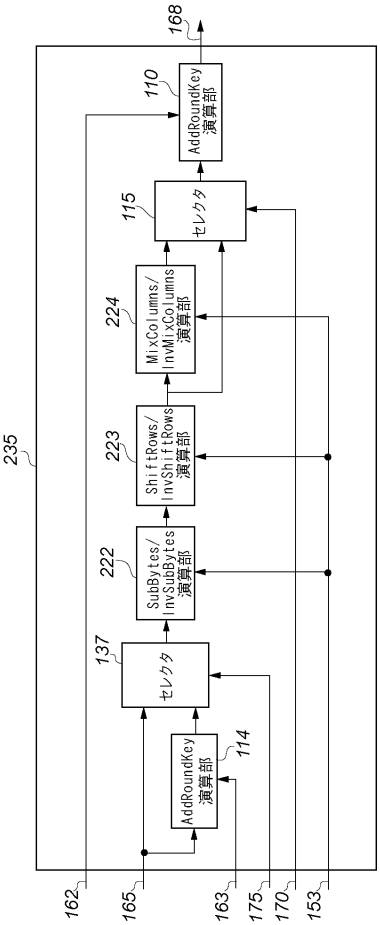
【図３８】



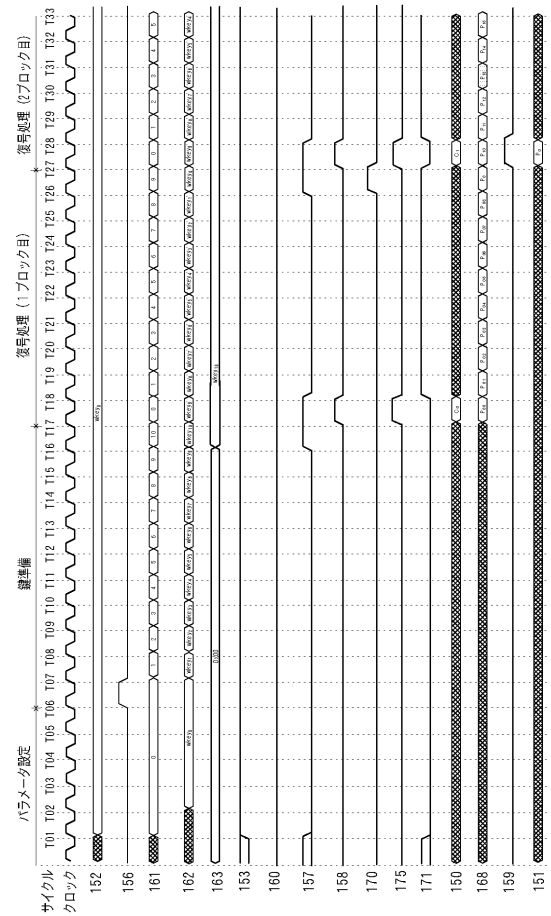
【図３９】



【図４０】



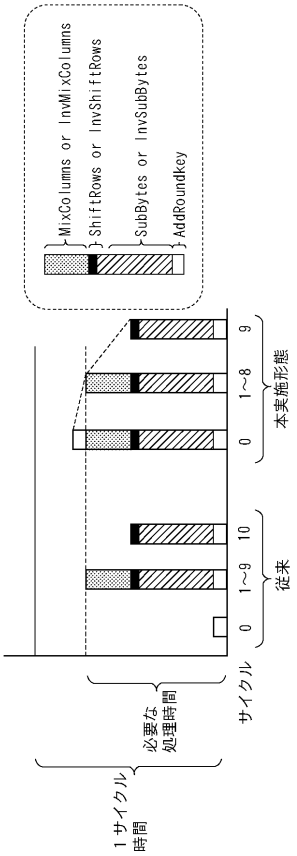
【図４１】



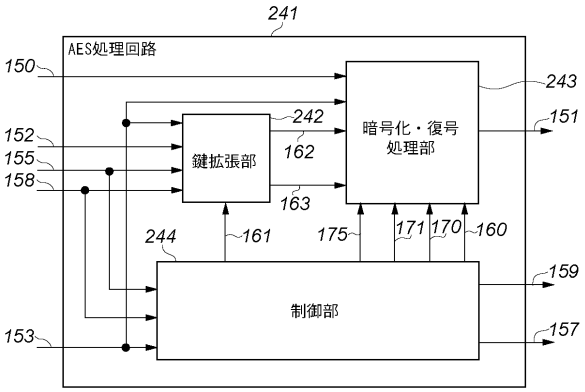
【図４２】

サイクル数	暗号化時の処理		復号時の処理	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey	•0番目の実行鍵 ($wkey_0$) •1番目の実行鍵 ($wkey_1$)	•AddRoundKey •InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•10番目の実行鍵 ($wkey_{10}$) •9番目の特殊実行鍵 ($wkey_9'$)
1	•SubBytes •ShiftRows •MixColumns •AddRoundKey	・2番目の実行鍵 ($wkey_2$)	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•8番目の特殊実行鍵 ($wkey_8'$)
8	•SubBytes •ShiftRows •MixColumns •AddRoundKey	•9番目の実行鍵 ($wkey_9$)	•InvSubBytes •InvShiftRows •InvMixColumns •AddRoundKey	•1番目の特殊実行鍵 ($wkey_1'$)
9	•SubBytes •ShiftRows •AddRoundKey	•10番目の実行鍵 ($wkey_{10}$)	•InvSubBytes •InvShiftRows •AddRoundKey	•0番目の実行鍵 ($wkey_0$)

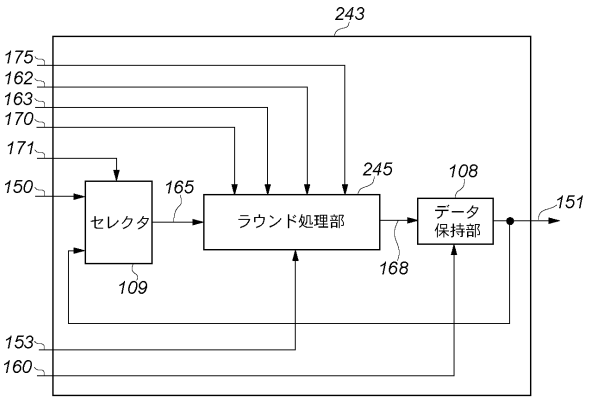
【図４３】



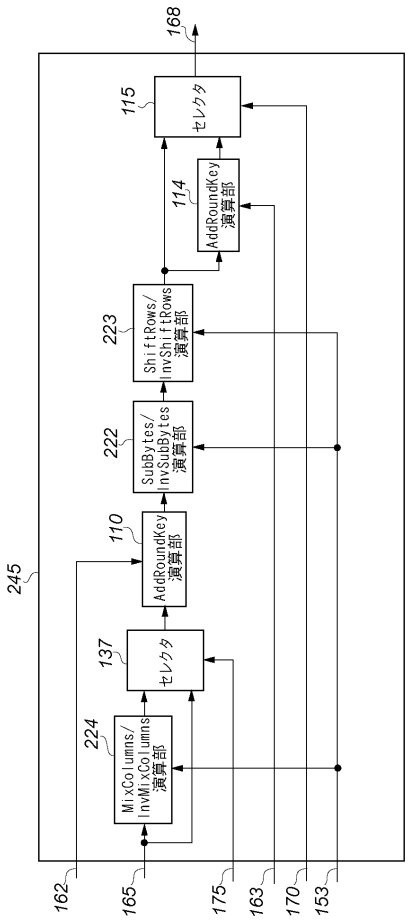
【図４４】



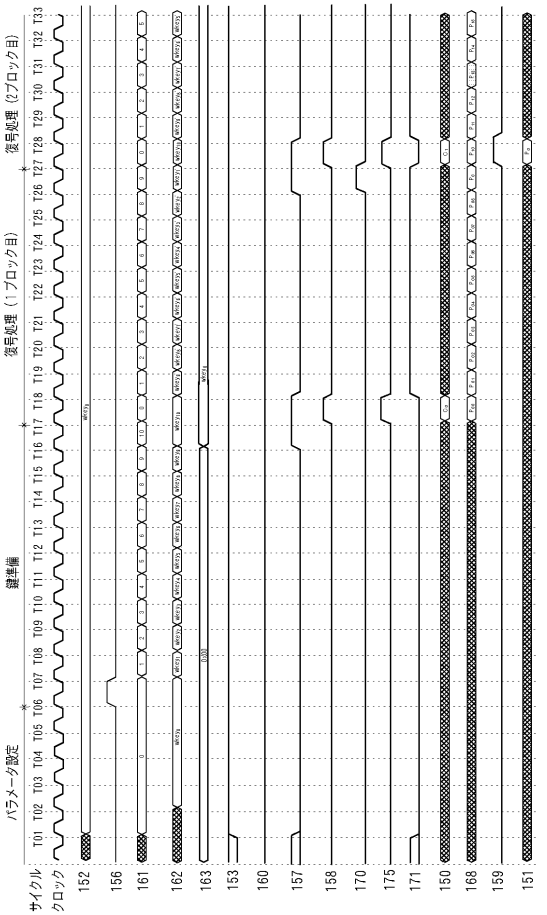
【図４５】



【図４６】



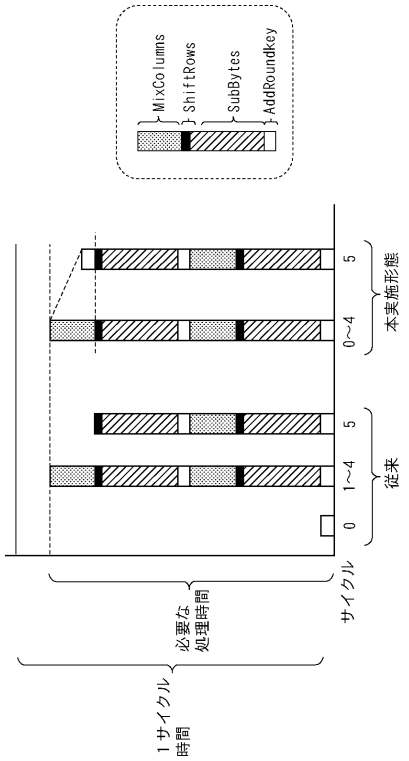
【図４７】



【図４８】

サイクル数	従来		実施形態７	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey	•0番目の実行鍵 ($wkey_0$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey •SubBytes •ShiftRows •MixColumns	•0番目の実行鍵 ($wkey_0$) •1番目の実行鍵 ($wkey_1$)
1	•SubBytes •ShiftRows •MixColumns •AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey	•1番目の実行鍵 ($wkey_1$) •2番目の実行鍵 ($wkey_2$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey •SubBytes •ShiftRows •MixColumns	•2番目の実行鍵 ($wkey_2$) •3番目の実行鍵 ($wkey_3$)
4	•SubBytes •ShiftRows •MixColumns •AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey	•7番目の実行鍵 ($wkey_7$) •8番目の実行鍵 ($wkey_8$)	•AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey •SubBytes •ShiftRows •AddRoundKey	•8番目の実行鍵 ($wkey_8$) •9番目の実行鍵 ($wkey_9$) •10番目の実行鍵 ($wkey_{10}$)
5	•SubBytes •ShiftRows •MixColumns •AddRoundKey •SubBytes •ShiftRows •AddRoundKey	•9番目の実行鍵 ($wkey_9$) •10番目の実行鍵 ($wkey_{10}$)		

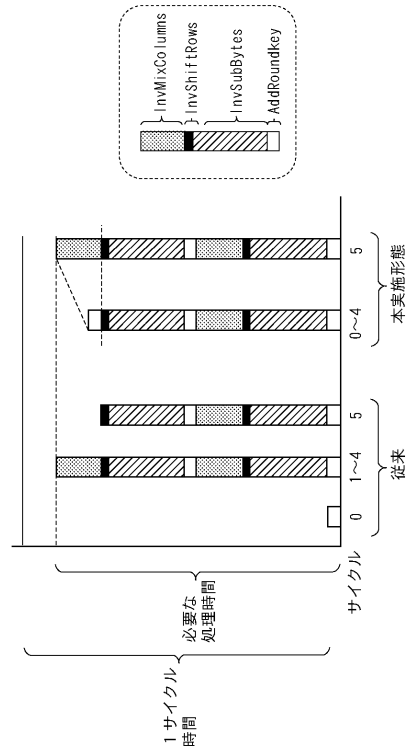
【図４９】



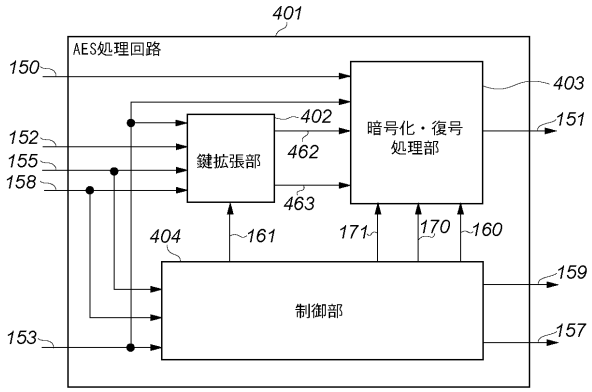
【図５０】

サイクル数	従来		実施形態７	
	実行される処理	使用する実行鍵	実行される処理	使用する実行鍵
0	•AddRoundKey	•10番目の実行鍵 ($wkey_{10}$)	•AddRoundKey •InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	•10番目の実行鍵 ($wkey_{10}$) •9番目の実行鍵 ($wkey_9$) •8番目の実行鍵 ($wkey_8$)
1	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	•9番目の実行鍵 ($wkey_9$) •8番目の実行鍵 ($wkey_8$)	•InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	•7番目の実行鍵 ($wkey_7$) •6番目の実行鍵 ($wkey_6$)
4	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns	•3番目の実行鍵 ($wkey_3$) •2番目の実行鍵 ($wkey_2$)	•InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	•1番目の実行鍵 ($wkey_1$) •0番目の実行鍵 ($wkey_0$)
5	•InvShiftRows •InvSubBytes •AddRoundKey •InvMixColumns •InvShiftRows •InvSubBytes •AddRoundKey	•1番目の実行鍵 ($wkey_1$) •0番目の実行鍵 ($wkey_0$)		

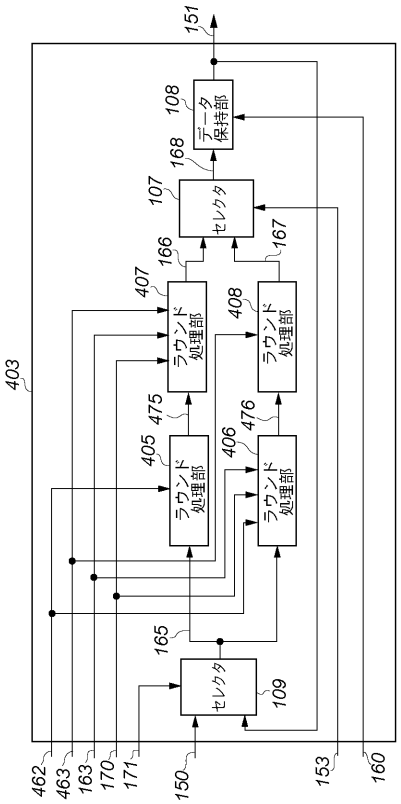
【図５１】



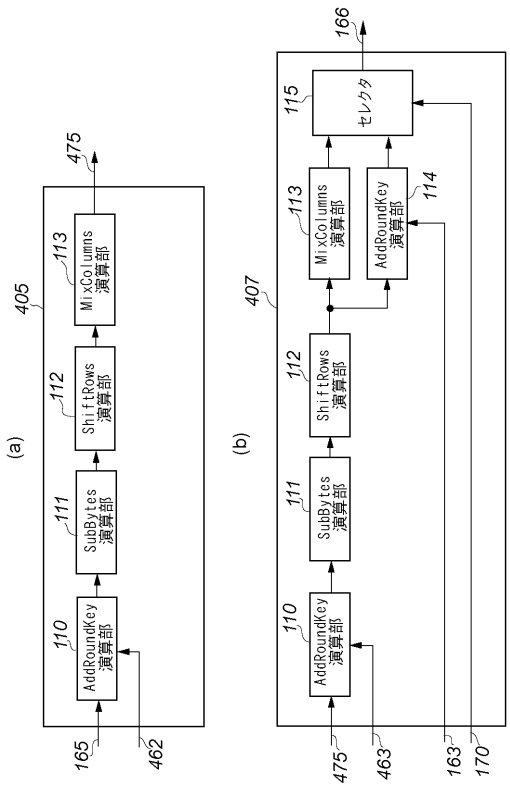
【図５２】



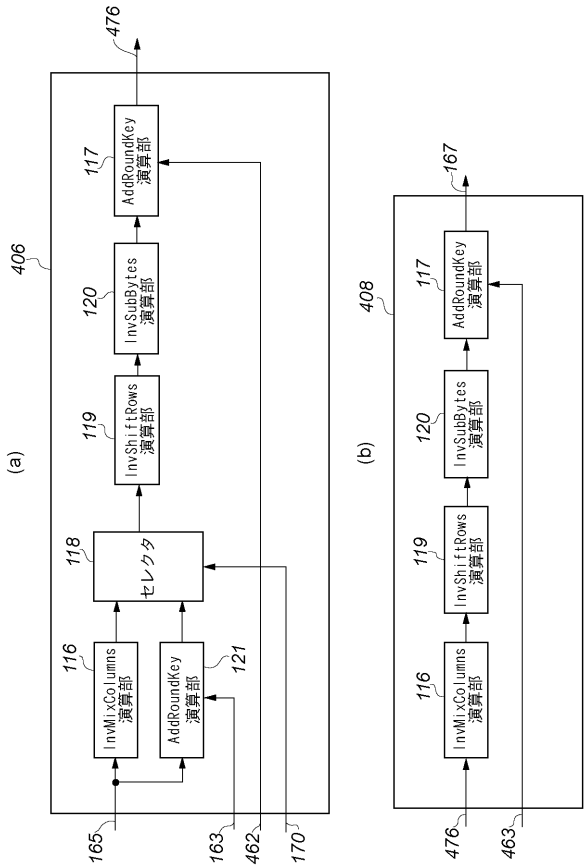
【図５３】



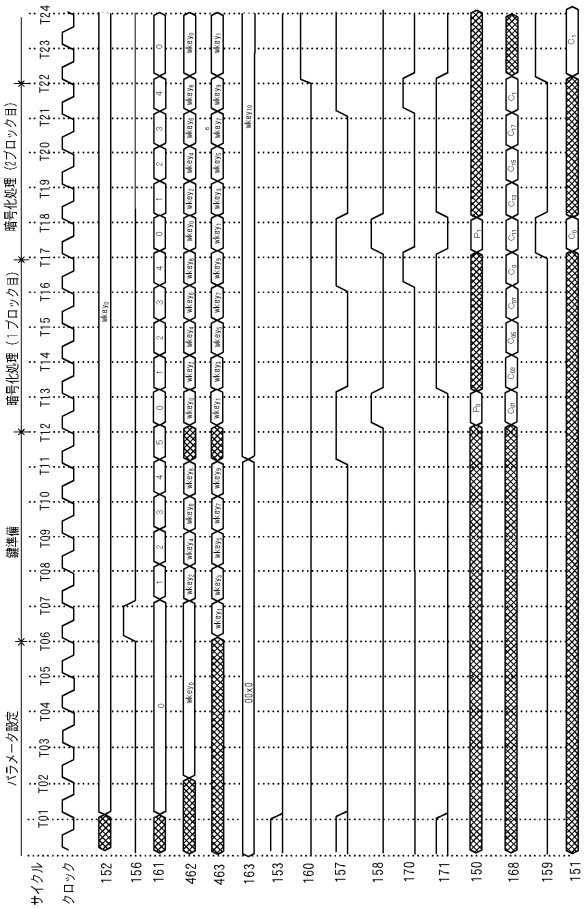
【図５４】



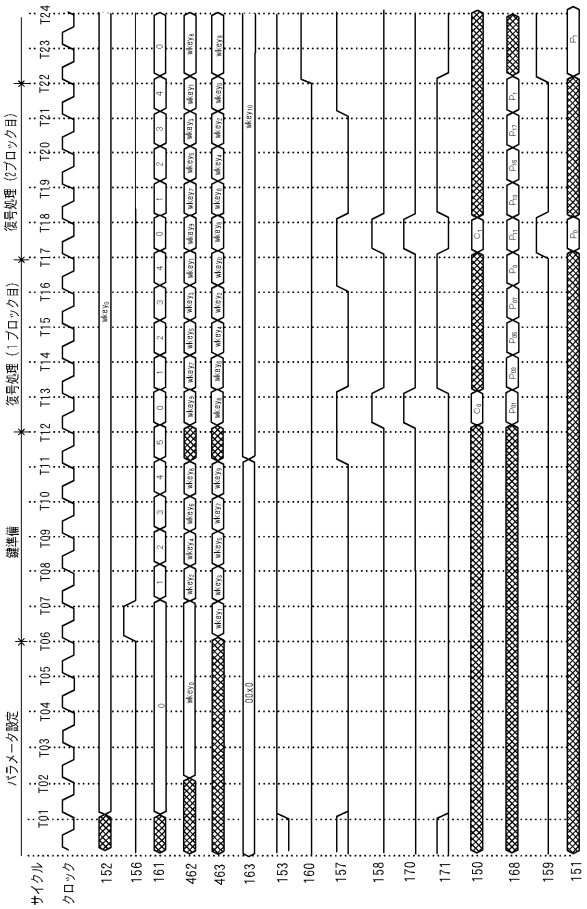
【図５５】



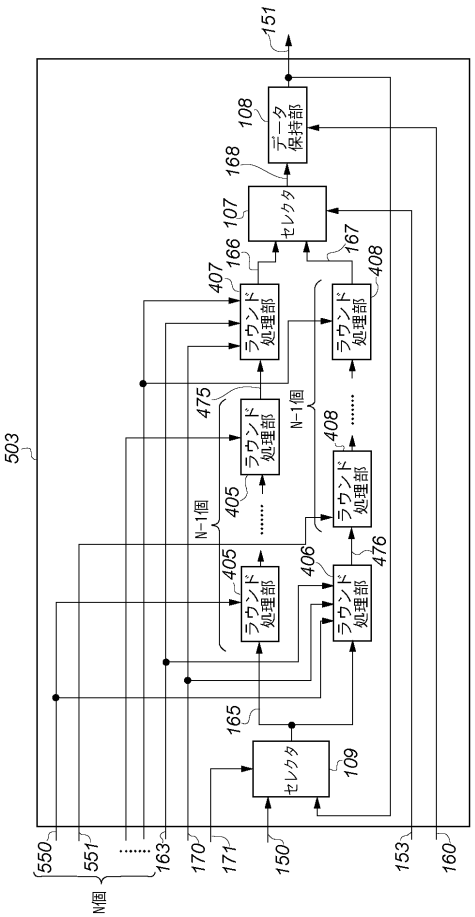
【図５６】



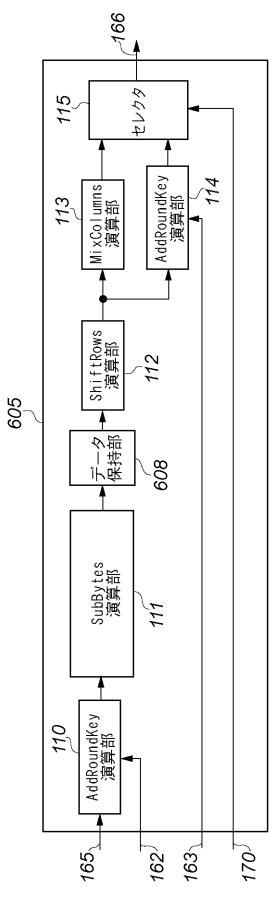
【図５７】



【図５８】



【図５９】



【図６０】

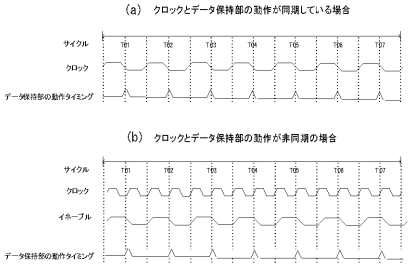
```
AddRoundKey ( )
For round = 1 step 1 to Nr-1
    InvShiftRows( )
    InvSubBytes( )
    AddRoundKey ( )
    InvMixColumns( )
End for
InvShiftRows( )
InvSubBytes( )
AddRoundKey( )
```

復号処理アルゴリズム

```
AddRoundKey ( )
For round = 1 step 1 to Nr-1
    SubBytes ( )
    ShiftRows ( )
    MixColumns ( )
    AddRoundKey ( )
End for
SubBytes( )
ShiftRows( )
AddRoundKey ( )
```

暗号化処理アルゴリズム

【図６１】



【図６２】

処理開始からのクロックサイクル数	暗号化時の処理	
	実行される処理	使用する実行鍵
0	•AddRoundKey •SubBytes •ShiftRows •MixColumns	•0番目の実行鍵 （$wkey_0$）
1	•AddRoundKey •SubBytes •ShiftRows •MixColumns	•1番目の実行鍵 （$wkey_1$）
7	•AddRoundKey •SubBytes •ShiftRows •MixColumns •AddRoundKey	•7番目の実行鍵 （$wkey_7$） •8番目の実行鍵 （$wkey_8$）
8	•SubBytes •ShiftRows •MixColumns •AddRoundKey	•9番目の実行鍵 （$wkey_9$）
9	•SubBytes •ShiftRows •AddRoundKey	•10番目の実行鍵 （$wkey_{10}$）

フロントページの続き

(72)発明者　堀田　博久
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
(72)発明者　熊取谷　昭彦
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　石田　信行

(56)参考文献　特表２００５－５２７８５３（ＪＰ，Ａ）
特開２００８－２０３３０６（ＪＰ，Ａ）
特開２００８－０４０２４４（ＪＰ，Ａ）
特表２００５－５３１０２３（ＪＰ，Ａ）
特開２００５－２１５６８８（ＪＰ，Ａ）
特開２００３－０１５５２２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／０６