【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成23年10月20日(2011.10.20)

【公開番号】特開2009-109988(P2009-109988A)
【公開日】平成21年5月21日(2009.5.21)
【年通号数】公開・登録公報2009-020
【出願番号】特願2008-233094(P2008-233094)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６１０Ａ

【手続補正書】
【提出日】平成23年9月2日(2011.9.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
AES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】

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４】

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MixColumns演算部に入力し、前記MixColumns演算部の出力を前記第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MixColumns演算部に入力し、前記MixColumns演算部の出力を前記第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５】

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乃至４の何れか１項に記載の暗号処理回路。

【請求項６】

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７】

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６に記載の暗号処理回路。

【請求項８】

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６に記載の暗号処理回路。

【請求項９】

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InvMixColumns演算部に入力し、前記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-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InvMixColumns演算部に入力し、前記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６に記載の暗号処理回路。

【請求項１０】

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６乃至９の何れか１項に記載の暗号処理回路。

【請求項１１】

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１２】

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暗号処理回路。

【請求項１３】

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１１又は請求項１２に記載の暗号処理回路。
【請求項１４】
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１５】
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暗号処理回路。
【請求項１６】
CipherKeyからRoundKeyを生成し、前記第１のAddRoundKey演算部、前記第２のAddRoun

dKey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１４又は請求項１５に記載の暗号処理回路。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】

上記課題を解決するため、本発明はAESの暗号化処理、復号処理を行う際に、各クロックサイクル内で実行する処理の処理時間を均等化する。そのため、例えば本発明に係る暗号処理回路は、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。