【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19年8月30日(2007.8.30)

【公開番号】特開2005-141198(P2005-141198A)
【公開日】平成17年6月2日(2005.6.2)
【年通号数】公開・登録公報2005-021
【出願番号】特願2004-274103(P2004-274103)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ａ

【手続補正書】
【提出日】平成19年7月18日(2007.7.18)
【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】
複数のデータを取得する取得手段と、
前記複数のデータの各々に対して、有限体ＧＦ（2^n）（ｎは自然数）上の値を係数とする多項式剰余環上における所定のべき数による、べき乗演算に基づく変換を行うべき乗手段と、
前記べき乗手段で変換された後の前記複数のデータに基づいて出力データを生成する出力データ生成手段とを備え、
前記所定のべき数は３以上であり、かつ2^m（ｍは１以上の整数）以外の値である
ことを特徴とするデータ変換装置。
【請求項２】
さらに、有限体ＧＦ（2^n）上の乗算を行なう有限体乗算手段を備え、
前記べき乗手段は、前記有限体乗算手段を利用してべき乗演算を行なう
ことを特徴とする請求項１に記載のデータ変換装置。
【請求項３】
前記べき乗手段は、
前記取得手段で取得された前記複数のデータの各々に対して、所定の定数との前記多項式剰余環上の加算を行なう加算部と、
前記加算部で加算後の前記複数のデータの各々に対して、前記多項式剰余環上における所定のべき数によるべき乗演算に基づく変換を行なうべき乗部とを有する
ことを特徴とする請求項１に記載のデータ変換装置。
【請求項４】
前記出力データ生成手段は、
前記べき乗手段で変換された後の前記複数のデータ同士で、前記多項式剰余環上の加算を行なう加算部と、
前記加算部の加算結果に対して所定の定数との前記有限体ＧＦ（2^n）上の乗算を行なう乗算部とを有する
ことを特徴とする請求項１に記載のデータ変換装置。
【請求項５】
さらに、有限体ＧＦ（2^n）上の乗算を行なう有限体乗算手段を備え、

前記べき乗手段は、前記有限体乗算手段を利用してべき乗演算を行ない、
前記乗算部は、前記有限体乗算手段を利用して乗算を行なう
ことを特徴とする請求項４に記載のデータ変換装置。
【請求項６】
複数のデータを取得する取得ステップと、
前記複数のデータの各々に対して、有限体ＧＦ（2^n）（ｎは自然数）上の値を係数とする多項式剰余環上における所定のべき数による、べき乗演算に基づく変換を行なうべき乗ステップと、
前記べき乗ステップで変換された後の前記複数のデータに基づいて出力データを生成する出力データ生成ステップとを含み、
前記所定のべき数は３以上であり、かつ2^m（ｍは１以上の整数）以外の値である
ことを特徴とするデータ変換方法。
【請求項７】
前記べき乗ステップでは、有限体ＧＦ（2^n）上の乗算を行なう有限体乗算手段を利用してべき乗演算を行なう
ことを特徴とする請求項６に記載のデータ変換方法。
【請求項８】
前記べき乗ステップは、
前記取得ステップで取得された前記複数のデータの各々に対して、所定の定数との前記多項式剰余環上の加算を行なう加算サブステップと、
前記加算サブステップで加算後の前記複数のデータの各々に対して、前記多項式剰余環上における所定のべき数によるべき乗演算に基づく変換を行なうべき乗サブステップとを含む
ことを特徴とする請求項６に記載のデータ変換方法。
【請求項９】
前記出力データ生成ステップは、
前記べき乗ステップで変換された後の前記複数のデータ同士で、前記多項式剰余環上の加算を行なう加算サブステップと、
前記加算サブステップの加算結果に対して所定の定数との前記有限体ＧＦ（2^n）上の乗算を行なう乗算サブステップとを含む
ことを特徴とする請求項６に記載のデータ変換方法。
【請求項１０】
前記べき乗ステップでは、有限体ＧＦ（2^n）上の乗算を行なう有限体乗算手段を利用してべき乗演算を行ない、
前記乗算サブステップでは、有限体ＧＦ（2^n）上の乗算を行なう有限体乗算手段を利用して乗算を行なう
ことを特徴とする請求項９に記載のデータ変換方法。
【請求項１１】
有限体ＧＦ（2^n）（ｎは自然数）上の乗算を行なう有限体乗算手段と、
前記有限体乗算手段を利用して有限体ＧＦ（2^n）上の乗算を行なうことにより入力データに対して誤り訂正符号化を行なう誤り訂正符号化手段と、
入力データを複数のデータに分割する分割手段と、
前記有限体乗算手段を利用して前記複数のデータの各々に対して、有限体ＧＦ（2^n）上の値を係数とする多項式剰余環上における所定のべき数による、べき乗演算に基づく変換を行なうべき乗手段と、
前記べき乗手段で変換された後の前記複数のデータに基づいて出力データを生成する出力データ生成手段とを備え、
前記所定のべき数は３以上であり、かつ2^m（ｍは１以上の整数）以外の値である
ことを特徴とする集積回路。
【請求項１２】

前記べき乗手段は、
前記分割手段で分割された後の前記複数のデータの各々に対して、所定の定数との前記多項式剰余環上の加算を行なう加算部と、
前記有限体乗算手段を利用して、前記加算部における加算後の前記複数のデータの各々に対して、前記多項式剰余環上における所定のべき数によるべき乗演算に基づく変換を行なうべき乗部とを有する
ことを特徴とする請求項１１に記載の集積回路。
【請求項１３】
前記出力データ生成手段は、
前記べき乗手段で変換された後の前記複数のデータ同士で、前記多項式剰余環上の加算を行なう加算部と、
前記有限体乗算手段を利用して、前記加算部の加算結果に対して、所定の定数との前記有限体ＧＦ（2^n）上の乗算を行なう乗算部とを有する
ことを特徴とする請求項１１に記載の集積回路。
【請求項１４】
複数のデータを取得する取得ステップと、
有限体ＧＦ（2^n）（ｎは自然数）上の乗算を行なう有限体乗算手段を利用して、前記複数のデータの各々に対して、有限体ＧＦ（2^n）上の値を係数とする多項式剰余環上における所定のべき数による、べき乗演算に基づく変換を行なうべき乗ステップと、
前記べき乗ステップで変換された後の前記複数のデータに基づいて出力データを生成する出力データ生成ステップとをコンピュータに実行させ、
前記所定のべき数は３以上であり、かつ2^m（ｍは１以上の整数）以外の値である
ことを特徴とするプログラム。
【請求項１５】
前記べき乗ステップは、
前記取得ステップで取得された前記複数のデータの各々に対して、所定の定数との前記多項式剰余環上の加算を行なう加算サブステップと、
前記有限体乗算手段を利用して、前記加算サブステップで加算後の前記複数のデータの各々に対して、前記多項式剰余環上における所定のべき数によるべき乗演算に基づく変換を行なうべき乗サブステップとを含む
ことを特徴とする請求項１４に記載のプログラム。
【請求項１６】
前記出力データ生成ステップは、
前記べき乗ステップで変換された後の前記複数のデータ同士で、前記多項式剰余環上の加算を行なう加算サブステップと、
前記有限体乗算手段を利用して、前記加算サブステップの加算結果に対して所定の定数との前記有限体ＧＦ（2^n）上の乗算を行なう乗算サブステップとを含む
ことを特徴とする請求項１４に記載のプログラム。