【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10月18日(2007.10.18)

【公開番号】特開2005-122141(P2005-122141A)
【公開日】平成17年5月12日(2005.5.12)
【年通号数】公開・登録公報2005-018
【出願番号】特願2004-269033(P2004-269033)
【国際特許分類】
*Ｇ０９Ｃ　1/00　(2006.01)*
*Ｇ０６Ｆ　7/72　(2006.01)*
*Ｇ０６Ｆ　9/38　(2006.01)*
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ａ
Ｇ０６Ｆ　7/72
Ｇ０６Ｆ　9/38　３７０Ａ

【手続補正書】
【提出日】平成19年9月4日(2007.9.4)
【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】
モンゴメリ乗算を実施するための処理システムにおいて、
１組のレジスタ（１０８）を有し、暗号化機能を実行するプロセッサであって、前記モンゴメリ乗算は、前記暗号化機能におけるべき乗を計算するために使用されるものであり、当該プロセッサがＳＩＭＤ命令をサポートするように構成されたプロセッサ（１０２）と、
モンゴメリ乗算を実行するための、前記プロセッサによって実行可能な１組のＳＩＭＤ命令（１１０）とを含む処理システムであって、
前記モンゴメリ乗算は、
ｍｏｎｔｍｕｌ（Ａ，Ｂ）＝ｒｅｍ（（ＡＢ－ｑＮ）／Ｒ，Ｎ）、ここでｑ＝ｒｅｍ（ＡＢ　Ｎ’，Ｒ）であり、
ＡおよびＢは整数であり、ｑは商であり、Ｎは法であり、Ｒは法Ｎと互いに素である整数であり、Ｎ’はＮＮ’≡１（ｍｏｄ　Ｒ）となるような整数であり、ｒｅｍは剰余演算であって、かつ、
前記整数Ｂおよび前記法Ｎは配列として実施され、少なくとも１つのＳＩＭＤ命令を使用して、ＡＢを計算するためのＢの倍数で第１の配列$Ｔ_1$を更新し、ｑＮを計算するためのＮの倍数で第２の配列$Ｔ_2$を更新するものとして定義されるものであり、
第１のレジスタは、前記ＢおよびＮの配列の要素を保持し、
第２のレジスタは、前記第１の配列$Ｔ_1$の要素と前記第２の配列$Ｔ_2$の要素とを保持し、
第３のレジスタは、Ｂの倍数で更新された前記第１の配列$Ｔ_1$およびＮの倍数で更新された前記第２の配列$Ｔ_2$の結果を保持するために使用されるものであり、
前記ＳＩＭＤ命令は、乗算ＡＢおよびｑＮの部分を同時に実行する単一のＳＩＭＤ命令を含む
ことを特徴とする処理システム。

【請求項２】
単一のＳＩＭＤ命令を使用して前記第１の配列$T_1$と前記第２の配列$T_2$とを同時に更新することを特徴とする請求項１に記載の処理システム。
【請求項３】
前記プロセッサ（１０２）は前記モンゴメリ乗算からの中間計算値を保持するための２つの配列を維持し、前記ＳＩＭＤ命令（１１２）を使用して前記２つの配列を同時に更新することを特徴とする請求項１または請求項２に記載の処理システム。
【請求項４】
前記モンゴメリ乗算は入力配列の第１の乗算と法配列の第２の乗算とを含み、前記ＳＩＭＤ命令（１１０）を使用して前記第１および第２の乗算を同時に実行することを特徴とする請求項１または請求項２に記載の処理システム。
【請求項５】
前記モンゴメリ乗算は命令のループを有し、前記ループの各反復は、コピー演算を除き８つ以下のＳＩＭＤ命令（１１０）を使用するステップを含むことを特徴とする請求項１または請求項２に記載の処理システム。
【請求項６】
前記ＳＩＭＤ命令（１１０）は、２つのロード命令と、１つの乗算命令と、２つの加算命令と、１つのコピー命令と、１つのビットごとのＡＮＤ命令と、１つのストア命令と、１つのシフト命令とを含むことを特徴とする請求項５に記載の処理システム。
【請求項７】
モンゴメリ乗算を実施するためのコンピュータ読み取り可能媒体において、
プロセッサ（１０２）上で実行されるとき、前記プロセッサにモンゴメリ乗算を実行するよう命令するコンピュータ実行可能なＳＩＭＤ命令（１１０）を備え、
前記プロセッサ（１０２）は、暗号化機能を実行するためのものであり、前記モンゴメリ乗算は、前記暗号化機能におけるべき乗を計算するために使用されるものであり、
前記モンゴメリ乗算は、
ｍｏｎｔｍｕｌ（Ａ，Ｂ）＝ｒｅｍ（（ＡＢ－ｑＮ）／Ｒ，Ｎ）、ここでｑ＝ｒｅｍ（ＡＢ　Ｎ’，Ｒ）であり、
ＡおよびＢは整数であり、ｑは商であり、Ｎは法であり、Ｒは法Ｎと互いに素である整数であり、Ｎ’はＮＮ’≡１（ｍｏｄ　Ｒ）となるような整数であり、ｒｅｍは剰余演算であって、かつ、
前記整数Ｂおよび前記法Ｎは配列として実施され、少なくとも１つのＳＩＭＤ命令を使用して、ＡＢを計算するためのＢの倍数で第１の配列$T_1$を更新し、ｑＮを計算するためのＮの倍数で第２の配列$T_2$を更新するものとして定義されるものであり、
第１のレジスタは、前記ＢおよびＮの配列の要素を保持し、
第２のレジスタは、前記第１の配列$T_1$の要素と前記第２の配列$T_2$の要素とを保持し、
第３のレジスタは、Ｂの倍数で更新された前記第１の配列$T_1$およびＮの倍数で更新された前記第２の配列$T_2$の結果を保持するために使用されるものであり、
前記ＳＩＭＤ命令は、乗算ＡＢおよびｑＮの部分を同時に実行する単一のＳＩＭＤ命令を含む
ことを特徴とするコンピュータ読み取り可能媒体。
【請求項８】
配列ＢおよびＮの要素を前記第１のレジスタにロードするための第１のＳＩＭＤ命令と、
配列$T_1$および$T_2$の要素を前記第２のレジスタにロードするための第２のＳＩＭＤ命令と、
第１の乗算による前記配列Ｂの要素と、第２の乗算による前記配列Ｎの要素とを乗算するための、第３のＳＩＭＤ命令と、
前記第２のＳＩＭＤ命令によってロードされた前記配列要素、および前回の反復から保

存された任意の桁上げ数に、前記第３のＳＩＭＤ命令の結果を加算するための、第４および第５のＳＩＭＤ命令と、
前記第５のＳＩＭＤ命令のそれぞれの出力を、１つは配列$T_1$および$T_2$に収まりもう１つは次の反復のための桁上げ数を表す２つの縮小された結果に分けるための第６および第７のＳＩＭＤ命令と、
メモリ内の、配列$T_1$の要素および配列$T_2$の要素を更新するための第８のＳＩＭＤ命令とを含むことを特徴とする請求項７に記載のコンピュータ読取り可能媒体。
【請求項９】
前記ＳＩＭＤ命令（１１０）はＳＳＥ２命令を含むものであることを特徴とする請求項７に記載のコンピュータ読取り可能媒体。
【請求項１０】
モンゴメリ乗算を実施する方法において、
モンゴメリ乗算を実行する際に使用される値で１組のレジスタ（１０８）を初期設定するステップであって、前記プロセッサ（１０２）は、暗号化機能を実行するためのものであり、前記モンゴメリ乗算は、前記暗号化機能におけるべき乗を計算するために使用されるものである、そのようなステップと、
前記レジスタ（１０８）に格納された前記値について、ＳＩＭＤ命令（１１０）を使用して前記モンゴメリ乗算を計算するステップと、を備え、
前記モンゴメリ乗算は、
ｍｏｎｔｍｕｌ（Ａ，Ｂ）＝ｒｅｍ（（ＡＢ－ｑＮ）／Ｒ，Ｎ）、ここでｑ＝ｒｅｍ（ＡＢ　Ｎ’，Ｒ）であり、
ＡおよびＢは整数であり、ｑは商であり、Ｎは法であり、Ｒは法Ｎと互いに素である整数であり、Ｎ’はＮＮ’≡１（ｍｏｄ　Ｒ）となるような整数であり、ｒｅｍは剰余演算であって、かつ、
前記整数Ｂおよび前記法Ｎは配列として実施され、少なくとも１つのＳＩＭＤ命令を使用して、ＡＢを計算するためのＢの倍数で第１の配列$T_1$を更新し、ｑＮを計算するためのＮの倍数で第２の配列$T_2$を更新するものとして定義されるものであり、
第１のレジスタは、前記ＢおよびＮの配列の要素を保持し、
第２のレジスタは、前記第１の配列$T_1$の要素と前記第２の配列$T_2$の要素とを保持し、
第３のレジスタは、Ｂの倍数で更新された前記第１の配列$T_1$およびＮの倍数で更新された前記第２の配列$T_2$の結果を保持するために使用されるものであり、
前記ＳＩＭＤ命令は、乗算ＡＢおよびｑＮの部分を同時に実行する単一のＳＩＭＤ命令を含む
ことを特徴とする方法。
【請求項１１】
前記計算するステップは、前記暗号化機能におけるべき乗を計算するために前記モンゴメリ乗算を使用するステップを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記計算するステップは、ＳＳＥ２命令を使用するステップを含むことを特徴とする請求項１０に記載の方法。
【請求項１３】
前記モンゴメリ乗算は命令のループを有し、前記ループの各反復は９以下のＳＩＭＤ命令を使用して実行されることを特徴とする請求項１０に記載の方法。
【請求項１４】
前記９つのＳＩＭＤ命令は、２つのロード命令と、１つの乗算命令と、２つの加算命令と、１つのコピー命令と、１つのビットごとのＡＮＤ命令と、１つのストア命令と、１つのシフト命令とを含むことを特徴とする請求項１３に記載の方法。
【請求項１５】
入力Ｂ×整数Ａの数字の積で配列$T_1$を更新し、更新された配列$T_1$、$T_2$を同じ前

記数字で終わらせることのできる法Ｎの倍数を決定するステップ、
　前記入力Ｂと前記整数Ａの数字を乗算し、前記法Ｎと前記決定された倍数とを乗算するステップ、および
　前記配列$Ｔ_1$、$Ｔ_2$を更新するステップを、
前記整数Ａの各数字について、右から左へと反復して実行するステップをさらに備えることを特徴とする請求項１０に記載の方法。
【請求項１６】
前記乗算するステップは、単一のＳＩＭＤ命令によって実行されることを特徴とする請求項１５に記載の方法。
【請求項１７】
前記実行するステップの前に、前記配列$Ｔ_1$、$Ｔ_2$および前記法Ｎを初期設定するステップをさらに備えることを特徴とする請求項１５に記載の方法。