(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-510998
(P2006-510998A)
(43)公表日　平成18年3月30日(2006.3.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660L	5B033
G06F 9/30	(2006.01)	G06F	9/30	310C	5B076
					5B276

審査請求 有　予備審査請求 有　（全 23 頁）

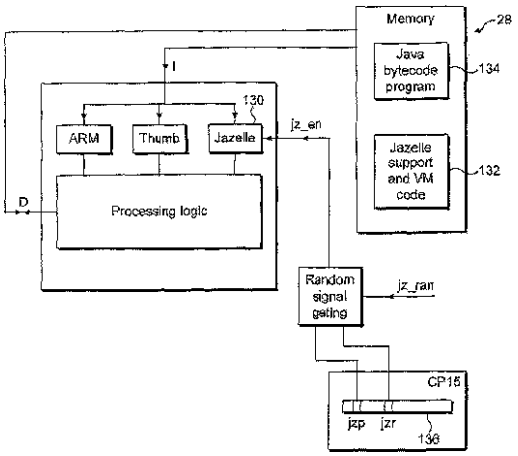
(21)出願番号	特願2005-502329 (P2005-502329)
(86)(22)出願日	平成15年10月6日 (2003.10.6)
(85)翻訳文提出日	平成17年3月22日 (2005.3.22)
(86)国際出願番号	PCT/GB2003/004313
(87)国際公開番号	WO2004/053684
(87)国際公開日	平成16年6月24日 (2004.6.24)
(31)優先権主張番号	0229068.2
(32)優先日	平成14年12月12日 (2002.12.12)
(33)優先権主張国	英国 (GB)
(31)優先権主張番号	0302650.7
(32)優先日	平成15年2月5日 (2003.2.5)
(33)優先権主張国	英国 (GB)
(31)優先権主張番号	0302646.5
(32)優先日	平成15年2月5日 (2003.2.5)
(33)優先権主張国	英国 (GB)

(71)出願人　594154428
エイアールエム　リミテッド
イギリス国　シービー１　９エヌジェイ
ケンブリッジ，チェリー　ヒントン，フルバーン　ロード　１１０
(74)代理人　100066692
弁理士　浅村　皓
(74)代理人　100072040
弁理士　浅村　肇
(74)代理人　100091339
弁理士　清水　邦明
(74)代理人　100094673
弁理士　林　鈺三

最終頁に続く

(54)【発明の名称】データ処理システム内の処理アクティビティのマスキング

(57)【要約】
データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための装置であって、データ処理命令の第一のセットを実行するように動作し得る第一の実行機構と、データ処理命令の第二のセットを実行するように動作し得る第二の実行機構であって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能であるように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、第二の実行機構と、前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択するように動作し得る実行機構選択器とを具備するデータ処理のための装置。



【特許請求の範囲】
【請求項１】
データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための装置であって、
データ処理命令の第一のセットを実行するように動作し得る第一の実行機構と、
データ処理命令の第二のセットを実行するように動作し得る第二の実行機構であって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能であるように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、第二の実行機構と、
前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択するように動作し得る実行機構選択器と、
を具備するデータ処理装置。
【請求項２】
請求項１に記載された装置であって、前記第一の実行機構と前記第二の実行機構とは、前記第一の実行機構または前記第二の実行機構によって実行可能である前記データ処理命令の少なくとも一つに対する少なくとも一つの異なる実行特性を備える、前記装置。
【請求項３】
請求項２に記載された装置であって、前記少なくとも一つの異なる実行特性は
前記データ処理命令を実行するための時間と、
前記データ処理命令を実行するときの電力消費
の一つ以上を含む、前記装置。
【請求項４】
請求項２と３のいずれか一つに記載された装置であって、前記第一の実行機構または前記第二の実行機構によって実行される少なくとも一つのデータ処理命令の少なくとも一つの実行特性が、先行するデータ処理命令が前記第一の実行機構または前記第二の実行機構で実行されたか否かに基づいて変動する、前記装置。
【請求項５】
先行する請求項のいずれか一つに記載された装置であって、前記データ処理命令のすべてが前記第一の実行機構または前記第二の実行機構によって実行可能である、前記装置。
【請求項６】
先行する請求項のいずれか一つに記載された装置であって、前記第一の実行機構は前記データ処理命令のいくつかを、データ処理ハードウェアを直接制御するネイティブ命令とエミュレーションソフトウェアを使用する残りのデータ処理命令として実行するように動作し得る、前記装置。
【請求項７】
先行する請求項のいずれか一つに記載された装置であって、前記第二の実行機構は、エミュレーションソフトウェアを使用する前記データ処理命令のすべてを実行するように動作し得る、前記装置。
【請求項８】
請求項６と７に記載された装置であって、前記第一の実行機構と前記第二の実行機構は少なくともいくつかのエミュレーションソフトウェアを共用する、前記装置。
【請求項９】
先行する請求項のいずれか一つに記載された装置であって、前記データ処理命令はジャバのバイトコード命令である、前記装置。
【請求項１０】
請求項９に記載された装置であって、前記第一の実行機構はネイティブのジャバのバイトコード実行ハードウェアを含み、前記第二の実行機構はすべてのジャバのバイトコードに対するジャバのバイトコードのエミュレーションを使用する、前記装置。
【請求項１１】

先行する請求項のいずれか一つに記載された装置であって、前記実行機構選択器は擬似ランダム実行機構選択信号によって制御される、前記装置。
【請求項１２】
請求項１１に記載された装置であって、プロセッサコアを具備し、前記擬似ランダム実行機構選択信号は前記プロセッサコアへの入力である、前記装置。
【請求項１３】
請求項１２に記載された装置であって、擬似ランダム信号発生器は前記擬似ランダム実行機構選択信号を発生するように動作し得る、前記装置。
【請求項１４】
先行する請求項のいずれか一つに記載された装置であって、前記実行機構選択器にすべてのデータ処理命令に対して前記第一の実行機構を選択させるようにシステム構成バラメータが動作し得る、前記装置。
【請求項１５】
請求項１４に記載された装置であって、前記システム構成バラメータがシステム構成レジスタに記憶される、前記装置。
【請求項１６】
データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための方法であって、
第一の実行機構でデータ処理命令の第一のセットを実行することと、
第二の実行機構でデータ処理命令の第二のセットを実行することであって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能であるように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、データ処理命令の第二のセットを実行することと、
前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、実行機構選択器で前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択することと、
からなる前記方法。
【請求項１７】
請求項１６に記載された方法であって、前記第一の実行機構と前記第二の実行機構とは、前記第一の実行機構または前記第二の実行機構によって実行可能である前記データ処理命令の少なくとも一つに対する少なくとも一つの異なる実行特性を備える、前記方法。
【請求項１８】
請求項１７に記載された方法であって、前記少なくとも一つの異なる実行特性は
前記データ処理命令を実行するための時間と、
前記データ処理命令を実行するときの電力消費
の一つ以上を含む、前記方法。
【請求項１９】
請求項１７と１８のいずれか一つに記載された方法であって、前記第一の実行機構または前記第二の実行機構によって実行される少なくとも一つのデータ処理命令の少なくとも一つの実行特性が、先行するデータ処理命令が前記第一の実行機構または前記第二の実行機構で実行されたか否かに基づいて変動する、前記方法。
【請求項２０】
請求項１６から１９のいずれか一つに記載された方法であって、前記データ処理命令のすべてが前記第一の実行機構または前記第二の実行機構によって実行可能である、前記方法。
【請求項２１】
請求項１６から２０のいずれか一つに記載された方法であって、前記第一の実行機構は前記データ処理命令のいくつかを、データ処理ハードウェアを直接制御するネイティブ命令とエミュレーションソフトウェアを使用する残りのデータ処理命令として実行するように動作し得る、前記方法。

【請求項２２】
請求項１６から２１のいずれか一つに記載された方法であって、前記第二の実行機構は、エミュレーションソフトウェアを使用する前記データ処理命令のすべてを実行するように動作し得る、前記方法。
【請求項２３】
請求項２１と２２に記載された方法であって、前記第一の実行機構と前記第二の実行機構は少なくともいくつかのエミュレーションソフトウェアを共用する、前記方法。
【請求項２４】
請求項１６から２３のいずれか一つに記載された方法であって、前記データ処理命令はジャバのバイトコード命令である、前記方法。
【請求項２５】
請求項２４に記載された方法であって、前記第一の実行機構はネイティブのジャバのバイトコード実行ハードウェアを含み、前記第二の実行機構はすべてのジャバのバイトコードに対するジャバのバイトコードのエミュレーションを使用する、前記方法。
【請求項２６】
請求項１６から２５のいずれか一つに記載された方法であって、前記実行機構選択器は擬似ランダム実行機構選択信号によって制御される、前記方法。
【請求項２７】
請求項２６に記載された方法であって、プロセッサコアを具備し、前記擬似ランダム実行機構選択信号は前記プロセッサコアへの入力である、前記方法。
【請求項２８】
請求項２７に記載された方法であって、擬似ランダム信号発生器は前記擬似ランダム実行機構選択信号を発生するように動作し得る、前記方法。
【請求項２９】
請求項１６から２８の請求項のいずれか一つに記載された方法であって、前記実行機構選択器にすべてのデータ処理命令に対して前記第一の実行機構を選択させるようにシステム構成バラメータが動作し得る、前記方法。
【請求項３０】
請求項２９に記載された方法であって、前記システム構成バラメータがシステム構成レジスタに記憶される、前記方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は処理システムの分野に関するものである。更に詳しくは、この発明は、たとえば、安全性向上のために、データ処理システム内の処理アクティビティをマスキングすることに関するものである。
【背景技術】
【０００２】
安全保証データを操作するデータ処理システムであって、また高度の安全性を確実にすることが望ましいデータ処理システムを提供することが知られている。たとえば、秘密の暗号化鍵のような安全保証データを操作するデータ処理システムを含むスマートカードを提供することが知られており、詐欺を防止するためにこのデータは秘密にしておかなければならない。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
このようなシステムの安全性を攻撃する知られている方法には、タイミング分析と電力分析が含まれる。入力に対するこのようなシステムのタイミング挙動（ｂｅｈａｖｉｏｕｒ）や電力消費挙動を観測することにより、遂行中の処理および操作中のデータに関する情報は、安全性を危うくし得る仕方で判定することができる。このような安全性攻撃に対

する抵抗を設けることは非常に有益である。
【課題を解決するための手段】
【０００４】
一側面から見ると本発明は、データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための装置であって、
データ処理命令の第一のセットを実行するように動作し得る第一の実行機構と、
データ処理命令の第二のセットを実行するように動作し得る第二の実行機構であって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能であるように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、第二の実行機構と、
前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択するように動作し得る実行機構選択器と
を具備するデータ処理のための装置を提供する。
【０００５】
本発明は、一つより多い実行機構によって実行され得る命令セットの少なくともいくつかの命令をそなえるシステム内で、それらの命令と関連付けられた電力シグネチャ（ｓｉｇｎａｔｕｒｅ）等の特性は、命令に対して異なる実行機構を擬似ランダム的に選択することによりマスクすることができるということを認識した。たとえば、ある命令を専用ハードウェアによってネイティブ実行してもよいし、ハードウェア上で動作する他のソフトウェアによってエミュレーションしてもよい場合には、この手法はこれらの機構の間で擬似ランダム的に切換えを行う。命令の実行と関連付けられた電力シグネチャを偽装するだけでなく、実行のタイミングも著しく変更される。
【０００６】
発明の好適実施例では、先行命令に対してどの実行機構が使用されたかに基づいて、命令と関連付けられた処理挙動が変更されるとき、処理挙動は有利な仕方で更に曖昧にされる。これが生じ得る理由については、たとえば、使用された前の実行機構に応じて、特定のデータまたは他の値がキャッシュ（ｃａｃｈｅ）されてもよく、キャッシュされなくてもよいので、本命令の実行に関連付けられた特性はその値がキャッシュされたか否かに応じて変動するからである。
【０００７】
実行すべき命令の中のいくつかだけが異なる実行機構によって実行できるときに本手法を使用できるが、実行すべき命令のすべてをいずれかの実行機構によって実行してもよいときには本発明の実現が簡略化される利点がある。こうして、実行機構の間の切換えは、当該特定の命令を考慮する必要はない。
【０００８】
命令の実行に関連付けられた非常に異なる特性を示す特定の好適実施例は、第一の実行機構では命令はハードウェアによってネイティブ命令として実行され、第二の実行機構では命令がソフトウェアによってエミュレーションされる実施例である。ネイティブハードウェア実行は通常、高速で、低消費電力であるが、ソフトウェアエミュレーションは比較的低速であり、高消費電力である。
【０００９】
実行機構が完全に相互に独立していることはあり得るが、それらがある程度重なり合うこともあり得る。本発明の好適実施例では、実行機構の一方はソフトウェアエミュレーションであり、他方の実行機構は、簡単な命令のネイティブハードウェアに基づく実行であり、より複雑な命令についてはソフトウェアエミュレーションを行う。より複雑な命令のソフトウェアエミュレーションは、両方の実行機構によって使用される共用ソフトウェアによって行うことができる。
【００１０】
異なる機構の作用を受け得る命令は様々な異なる形式をとり得るが、本発明は特に、バ

ーチャルマシン環境に関連付けられた命令、たとえば、ジャバ（登録商標）のバイトコードに特に適している。この環境では、第一の実行機構はジャバのバイトコードの中の少なくともいくつかのバイトコードのネイティブハードウェア実行でよく、他のジャバのバイトコードは、ジャバのバイトコードのすべてのソフトウェアエミュレーションである第二の実行機構で、ソフトウェアエミュレーションされる。

【００１１】

本手法はマイクロプロセッサに基づくシステム、ディジタル信号処理システム等のような様々なデータ処理システムに適用可能であるが、プロセッサコア実行プログラムを含むシステムであって、擬似ランダム信号が入力されて異なる実行機構間の選択が行われ、少なくともいくつかの命令に対する一つより多い実行機構を含むシステムに特に適している。

【００１２】

命令の実行特性を外部観測からマスクするために、このような命令に対して使用される実行機構について擬似ランダム選択を行うことができる。これらの命令はジャバのバイトコードであってもよく、ネイティブハードウェア実行とソフトウェアエミュレーションの混合である実行機構と全体がソフトウェアエミュレーションである実行機構との間で選択を行ってもよい。

【００１３】

安全性より効率が重要であるときには、実行機構の擬似ランダム選択をシステム構成パラメータによって選択的にイネーブル、ディスエーブルすることにより、最も効率的な実行機構の使用が強制されるようにしてもよい。

【実施例】

【００１４】

次に、付図を参照して本発明の実施例の説明を行うが、これらの実施例は例を示すに過ぎない。

【００１５】

図１は、プロセッサコア４、コプロセッサ６、およびメモリ８を含むデータ処理システム２を示す。

【００１６】

動作については、プロセッサコア４はメモリ８から命令とデータをフェッチする。命令は命令パイプライン１０に与えられ、そこで命令は、相次ぐ処理サイクル上のたとえば、フェッチ、復号、実行、メモリ、および書き戻しのような相次ぐパイプライン段を占める。パイプライン状のプロセッサはそれら自身、プロセッサ性能を改善するために、部分的に重なる仕方で多数のプログラム命令を有効に実行する仕方として周知である。

【００１７】

プロセッサコア４によってメモリ８から読み出されたデータ値はレジスタバンク１２に与えられる。レジスタバンク１２からのデータ値は、乗算器１４、シフタ１６、および加算器１８の一つ以上を使用してプログラム命令制御下で処理し得る。他のデータ処理回路、たとえば、ＡＮＤ、ＯＲ、先行ゼロ計数のような論理動作を行う回路を設けてもよい。

【００１８】

図１はプロセッサコア４内の命令復号器２０も示す。命令復号器２０は命令パイプライン１０内のプログラム命令に応答して実行制御信号を発生する。遂行されるデータ処理動作を制御するために、実行制御信号はレジスタバンク１２、乗算器１４、シフタ１６、および加算器１８のような種々の処理要素に与えられる。たとえば、復号器２０が発生する制御信号により、適当なオペランドがレジスタバンク１２から読み出されて、乗算器１４、シフタ１６、および加算器１８の中の適切なものの作用を受け、それにより発生した結果はレジスタバンク１２に書き戻される。

【００１９】

コプロセッサ６は多数の構成レジスタ２２を含むシステム構成コプロセッサであり、構成レジスタ２２はプログラム制御下で書き込まれて、構成制御パラメータを設定し得る。

これらの構成制御パラメータは、処理システム２の構成の多数の側面、たとえば、耐久性（ｅｎｄｉａｎｅｓｓ）等を指定することができる。これらの構成制御レジスタ２２の中の一つのレジスタに含まれているのは、プロセッサコアが固定タイミングモードまたは可変タイミングモードで動作すべきか否かを指定するビットである。このビットは命令復号器２０への入力として与えられるものとして示されているが、このビットを必要に応じてプロセッサコア４内の他の種々の点に供給して、それらの挙動を制御してもよいことは理解されよう。この固定／可変ビットに応じて、プロセッサコア４が固定タイミングモードまたは可変タイミングモードで動作する。固定タイミングモードにあるとき、可変タイミングモードで可変タイミングをそなえる（すなわち、完了に可変数の処理サイクルを要する）少なくとも一つのプログラム命令は、それを全体的に抑圧し得たか、または最大数より少ない処理サイクルで完了し得たか否かにかかわらず、その代わりに固定タイミングをそなえる（たとえば、完了に可能な最大数の処理サイクルを要する）ように強制される。命令復号器２０は主として、プログラム命令の復号とプロセッサコア４の他の要素のアクティビティを命令する責任があるので、命令復号器２０はプロセッサコア４を制御して固定タイミングモードで動作させるか、または可変タイミングモードで動作させる際に主要な役割を果たすことができる。すべての可変タイミング命令に固定タイミングモード型の動作を行わせる必要はない。

【００２０】

上記の説明で、構成制御レジスタ２２内の単一ビットは固定タイミングモードと可変タイミングモードとの間の切換えとして示されていることが理解されよう。その代わりに、構成制御レジスタ２２内の多重ビットを設けて、異なる型の命令の固定タイミングまたは可変タイミングの挙動、たとえば、条件付き命令の挙動、一様な分岐挙動、早期終了のディスエーブル、を別々にイネーブルまたはディセーブルしてもよい。

【００２１】

図２は条件付き命令２４の概略図である。この条件付き命令は、いくつかの条件付き命令だけを含む命令セットの一部、または実質的に完全な条件付きである、ＡＲＭ命令セットのような命令セットの一部であってもよい。条件コード２６はプロセッサ状態条件のセットを符号化し、その中で関連付けられた命令は実行されることもあり、実行されないこともある。たとえば、システムに現在設定されている条件コードがゼロの結果、けた上げが生じた、オーバフローが生じた等を示している場合には命令２４が実行しないと指定するように条件コード２６を構成することができる。この型の命令を使用して、効率的なプログラムコーディングを行うことができる。固定／可変ビットは少なくとも部分的に条件付き挙動を抑圧し、命令がそれの条件コードにかかわらず実行するが、プロセッサ状態に影響を及ぼす仕方でその結果を書き込まないことがあり得る。

【００２２】

図３は、命令復号器２０によって遂行される処理動作の一部の概略を示すフロー図である。図３はこれらの処理動作を論理シーケンスとして示すが、実際には少なくとも部分的には並列に、または異なる順序で遂行してもよいことは理解されよう。

【００２３】

ステップ２８で、命令復号器２０は新しい命令の実行を待つ。新しい命令を受けると、処理はステップ３０へ進み、そこで新しい命令と関連付けられた条件コードが読み取られる。ステップ３２で、これらの条件コードはシステム内に現在存在する条件コードと比較される。システム内に現在存在するこれらの条件コードは、これらの条件コードを更新した直前の命令または最後の命令での、前の処理アクティビティの結果である。

【００２４】

ステップ３４で、実行されつつある現在の命令の条件コード２６と既存の条件コードが合致するかチェックが行われる。合致しない場合には、処理はステップ３６に進んで、現在の命令の実行が開始される。図３は合致しないときに実行が行われるシステムを示しているが、合致するときに実行が行われるシステムも代わりの実施例となり得ることは理解されよう。

【００２５】
ステップ３６に続いて、処理はステップ３８に進み、命令の早期終了が可能か否かチェックが行われる。この早期終了はたとえば、オペランドの一つが０または１のような特定の値をそなえていることによるか、または特定の部分的な結果が作成された次の処理サイクルで行われる。早期終了が可能である場合には、処理がステップ４０に進み、プロセッサコア４が現在固定または可変タイミングモードで動作しているか否かについてチェックが行われる。プロセッサが可変タイミングモードにある場合には、処理がステップ４２に進み、当該命令が早期終了され、結果は適当なものとして戻され、処理はステップ２８に戻る。

【００２６】
ステップ４０での判定によりシステムが固定タイミングモードにある場合には、早期終了が可能である事実にかかわらず、処理がステップ４４に進む。ステップ３８で早期終了が可能でないと判定された場合にもステップ４４に進み、１処理サイクルの間、当該命令を実行する。乗算、除算、加算、または減算のような多サイクル処理命令の場合には、これらは実行に通常、数サイクルを要するので、ステップ４４の後、処理はステップ４６に進み、その命令に関連付けられた最大数のサイクルが既に遂行されたか否かの判定が行われる。最大数のサイクルが遂行された場合には、結果が発生されているはずである。早期終了が可能で、システムが更に数処理サイクルの間、実行し続けるように強制されている場合には、その型の命令に対する可能な最大数の処理サイクルに達したときにこの強制された実行は中止すべきであるということをステップ４６はまだ表示する。最大数の処理サイクルがまだ遂行されていない場合には、処理はステップ３８に戻される。

【００２７】
ステップ３４で試験した結果合致していれば、処理はステップ４８に進む。この例では、ステップ３４で合致していることが検出されると、これは特定の命令の実行を抑圧すべきであるということを示す。ステップ４８では、システムが現在、強制実行モードにあるか否か判定する。強制実行モードにある場合には、処理はステップ５０に進み、その命令の強制ダミー実行が行われる。ダミー実行が行われるとき、結果は命令自体に指定された行き先ではなくて、トラッシュレジスタ（図１のトラッシュレジスタ５１参照）に書き込まれる。これは、電力消費を実質的に変えないまま抑圧されるべきであったので、実行されるべきでなかったプログラム命令によってシステムの状態が修正されるのを防ぐためである。ステップ４８でシステムが強制実行モードになくて、可変タイミングモードにあると判定された場合には、処理はステップ５０をバイパスして、ステップ２８に戻り、プログラム命令が正規の仕方で抑圧される。

【００２８】
条件コードに符号化となったすべての命令にダミー実行が適用され、命令のすべての早期終了が抑圧される一般的なシステムを図３が示すことは理解されよう。実際上は、これらの手法を条件付き命令および早期終了が可能な命令のサブセットに適用することも可能である。上記の多重構成制御ビットを使用して、早期終了抑圧のような特徴を選択的にターンオンするが、条件コード不合格に続くダミー実行のような他の特徴はターンオンしないようにできる。

【００２９】
図４は、固定タイミングモードでの条件付き分岐命令の実行の概略図である。条件付き分岐命令ＢＥＱ（ｂｒａｎｃｈ　ｕｐｏｎ　ｅｑｕａｌ）に達するまで、一連の命令ＡＢが実行される。前の処理からの等しい結果を示すフラグがセットされている場合には指定された分岐が遂行され、フラグがセットされている場合には指定された分岐が抑圧されるという挙動をこの命令は符号化する。条件コードが合格したとき、すなわち、条件コードが合致したとき、分岐が行われ、処理が命令Ｘ、Ｙ等に進む。条件コードが不合格になった場合には、全体として抑圧される代わりに、ＢＥＱ命令は直後の命令Ｃに分岐する。これは、ＢＥＱ命令が抑圧され、まったく実行されない場合に到達するのと同じ命令である。しかし、固定タイミングモードでは、条件コードが合格するか不合格になるかにかかわ

らず、同数の処理サイクルを費やしてＢＥＱが実行される。これは、安全保証データにアクセスしようとする者から、前に遂行されたデータ処理動作の結果を隠す助けとなる。

【００３０】

図５はプログラム命令Ｉに応答して、データＤの処理を行うプログラマブルプロセッサコアの形式のデータ処理システム５２の概略図である。データ処理システム５２は、レジスタバンク５４、乗算器５６、シフタ５８、加算器６０、演算論理ユニット６２、ロードストアユニット６４、データパイプライン６６、命令復号器６８、およびランダムクロックゲーティング回路７０を含む。システム構成コプロセッサ（ＣＰ１５）７２がプロセッサコアに結合される。システム構成コプロセッサ７２はシステム構成レジスタ７４を含む。システム構成レジスタ７４は、それぞれデータ処理システム５２の異なる回路部分の擬似ランダムダミーアクティビティをイネーブルまたはディセーブル役目を果たす多重フラグ値を保持する。データ処理システム５２は通常、他の多数の回路要素を含むが、これらはわかりやすくするために図５では省略されている。

【００３１】

ダミーアクティビティイネーブル回路７６が乗算器５６に関連付けられ、乗算器５６の中のダミーアクティビティを適当としてイネーブルするか、またはその代わりに、実行されつつあるプログラム命令が要求したときに要求されたアクティビティイネーブル信号を通過させて乗算器５６を活性化する役目を果たす。同様のダミーアクティビティイネーブル回路７８、８０、８２、８４が前記の他の回路部分５８，６４、６２、６０に関連付けられている。

【００３２】

動作については、実行されるべき命令は命令パイプライン６６に、更に命令復号器６８に送られて、命令で駆動されるイネーブル信号を発生し、これらのイネーブル信号がそれぞれの回路部分に印加される。これらのイネーブル信号はデータ処理システム５２を通るデータ経路を選択し、当該回路部分を活性化することにより、それらの入力を読み取り、指定された処理を行い、それらの関連付けられた出力信号を発生する。たとえば、乗算－累積動作によって、レジスタバンク５４からデータ値が読み出され、これらのデータ値が乗算器５６および加算器６０に印加された後、結果がレジスタバンク５４に書き戻される。したがって、レジスタバンク５４、乗算器５６、および加算器６０はすべて、それらの動作をイネーブルすることと、それらを選択して完全なデータ経路を形成することの両方を行った必要なアクティビティイネーブル信号を受ける。回路部分が異なれば、電力消費特性とタイミング特性が異なるので、外部での観測でこのようなパラメータを観測することにより、どの命令が実行されつつあるかを明らかにすることができる。したがって、実行されつつある命令に必要とされない他の回路部分の擬似ランダムダミーアクティビティもイネーブルされる。したがって、実行されつつある特定の乗算－累積命令によってシフタ５８が使用されていなくても、その入力に印加される値をシフトすることにより電力を消費するようにシフタ５８を擬似ランダムイネーブルされることがある。それの出力ラッチはイネーブルされない。これは、このダミーアクティビティが望ましくない仕方で回路状態を変更して所要の動作を妨げること、たとえばいくつかの回路部分が出力値を持続することを避けるためである。当該回路部分に対する正規動作タイミングに合致する期間の間、ダミーアクティビティはイネーブルされる。

【００３３】

ランダムクロックゲーティング回路７０は、異なるそれぞれの回路部分に対する複数の擬似ランダムイネーブル信号を受信し、システム構成コプロセッサ７２内のシステム構成レジスタ７４から読み出される構成パラメータの制御下でこれらの擬似ランダムイネーブル信号をゲーティングして、それぞれの回路部分に印加する役目を果たす。これらの構成フラグは、シフタ５８、ＡＬＵ６２、および乗算器５６に対してはダミーアクティビティをイネーブルすべきであるが、加算器６０またはロードストアユニット６４に対してはダミーアクティビティをイネーブルすべきでないということを示すことがあり得る。異なる擬似ランダムイネーブル信号によって、これらのそれぞれの当該回路部分に合致し得る仕

方で異なる擬似ランダム特性を適用することができる。たとえば、異なる回路部分の正規タイミングに関連付けられた異なる最小イネーブル時間があってもよい。

【００３４】

総合的レベルでは、命令復号器６８は、現在実行されつつある命令によって指定されたデータ処理動作を行うために必要な回路部分をイネーブルする所要のアクティビティイネーブル回路としての役目を果たすことがわかる。この所要のアクティビティに重畳して、データ処理システム５２の残りの中の種々の場所に設けられたダミーアクティビティ制御回路によって、他の回路部分の中の種々のダミーアクティビティがイネーブル／刺激される。ダミーアクティビティは、所要のアクティビティに関連付けられた電力消費およびタイミング特性をマスクする役目を果たす。

【００３５】

図６は、所要のイネーブル信号ｅｎとダミーイネーブル信号ｒｎｄの両方を受け得る回路部分８６の概略図である。この回路部分８６は、それらの間で処理論理がデータ値を処理する一連のラッチとして考えることができる。真正の所要アクティビティが必要なとき、回路部分８６を通るデータ経路を提供するラッチのすべてはイネーブルされ、入力ラッチと出力ラッチとの間で所要処理が行われる。ダミーアクティビティが命令されたとき、入力ラッチと中間ラッチのみがイネーブルされる。したがって、回路部分全体を通してデータ経路が設けられず、その回路部分によって発生された出力値は変更されない。

【００３６】

図７は、擬似ランダムクロック信号を発生するために使用され得る型の線形帰還シフトレジスタを示す。これらのクロック信号は、図５のランダムクロックゲーティング回路７０に与えることができる。異なる回路部分に対して、別々の擬似ランダム信号発生器を設けてもよい。異なる擬似ランダム発生器に関連付けられた固定クロック周波数は、当該回路部分の特性と合致し、必要に応じてマスキング動作を更におおい隠すように変更してもよい。

【００３７】

図８は、ある回路部分に対するイネーブル信号の制御の概略図である。ステップ８８で、命令復号器６８からイネーブル信号ｅｎを受信したか否かについての判定が行われる。このようなイネーブル信号を受信した場合には、処理はステップ９０に進む。命令復号器６８からのイネーブル信号は、復号されつつある真正のプログラム命令に従って所要処理動作が必要であるということを示す。したがって、ステップ９０は、当該回路部分への入力、出力、およびクロック信号をイネーブルする。ステップ８８で命令復号器からイネーブル信号ｅｎが受信されなければ、処理はステップ９２に進み、その回路部分のダミー動作が許可されるか否かについての判定が行われる。ダミー動作が許可されれば、処理はステップ９４に進み、その回路部分への入力およびクロックがイネーブルされるが、その回路部分からの出力はイネーブルされない。次に、その回路部分はダミーアクティビティに着手する。システム構成パラメータによって示されるように、ステップ９２でダミー動作が許可されないと判定されれば、ステップ９４に進むことにより処理は終了する。

【００３８】

図８に示されたプロセスは逐次フロー図の形式になっていることが理解されよう。実際上、この制御は別のシーケンスで遂行してもよく、データ処理システム５２全体に広がった回路要素を使用してもよい。逐次遂行されるものとして図示された動作は実際には、並列に遂行してもよいし、あるいは制御機能を修正してもよい。全体的なレベルで、個々の回路部分は適当なプログラム命令に応答してそれの正規の所要動作を遂行するようにイネーブルされ、また関連付けられた構成パラメータによって許可されたときダミーアクティビティを遂行するようにイネーブルされる。

【００３９】

図９はレジスタバンク９６の概略図である。このレジスタバンクは、ＡＲＭ社（英国ケンブリッジ）によって設計されたプロセッサによるユーザモードの動作に対するＡＲＭプロセッサプログラマモデルに基づく。実際上、他のプロセッサモードに対して他のレジス

タを設けてもよいが、わかりやすくするためにこれらは省略されている。データ値を保持するために、標準的なデータレジスタＲ０からＲ１５が設けられる。レジスタＲ１３、Ｒ１４、およびＲ１５は通常、プログラムカウンタ値、分岐リターンアドレス値、およびスタックポインタを記憶する役目を果たし、これらは安全性に関連しないデータ値となる傾向がある。したがって、Ｒ１３、Ｒ１４、およびＲ１５に対しては、データ書き込みについての遷移平衡は必要でない。条件コードに合格しない条件付き書き込みに関連した使用のためにレジスタバンク９６の中にトラッシュレジスタＲＴが設けられるので、その条件コードに合格しない条件付き書き込み命令は通常、書き込みを行わない。しかし、このシステムでは、条件コードが合格しなくても、このような合格しなかった条件付き書き込み命令はデータ値をトラッシュデータレジスタＲＴに書き込む。これにより、条件付き書き込み動作の条件コード不合格または条件コード合格に関連付けられる電力消費またはタイミングのどんな差もマスクされる。トラッシュデータレジスタＲＴは、命令内でオペランドを指定するレジスタでアドレス指定できる仕方でプログラマのモデルに現れない。

【００４０】

トラッシュデータレジスタＲＴとともに、高から低への、そして低から高への遷移を平衡させる目的で、レジスタ９８、１００も設けられる。トラッシュデータレジスタＲＴとともに、データレジスタＲ０からＲ１２について専用のダミーレジスタ９８が設けられる。遷移平衡手法を受けるデータレジスタへの各書き込みに応答して、排他的ＯＲ値とともに排他的ＯＲ値の反転値を記憶するために共用ダミーレジスタ１００が設けられる。レジスタ書き込み制御回路１０２は、データレジスタへのデータ値書き込みに応答して、他のレジスタ９８、１００に書き込まれるべき適当なデータ値を発生する役目を果たす。システム構成コプロセッサ７２からの適当なシステム構成制御フラグ信号によって選択的にイネーブル、ディセーブルされる。

【００４１】

図１０は、レジスタ書き込み制御回路１０２の動作の概略を示すフロー図である。ステップ１０４で、回路はレジスタ書き込み動作が命令されるのを待つ。ステップ１０６で、このレジスタ書き込みは、対称書き込み制御システムが適用されるデータレジスタの中の一つに行われるか、トラッシュデータレジスタＲＴに行われるかが判定される。レジスタ書き込みがこのようなレジスタに対して行われない場合には、処理はステップ１０８に進み、レジスタＲ１３、Ｒ１４およびＲ１５の中の一つに対して、所要データ値Ｘの単なる書き込みが行われる。

【００４２】

それに書き込みが行われつつあるレジスタが可能性として対称レジスタ書き込みを受ける場合には、ステップ１１０はこの特徴が現在イネーブルされるか否か判定する役目を果たす。この特徴が現在イネーブルされない場合には、処理はステップ１０８に進む。この特徴がイネーブルされる場合には、処理はステップ１１２に進む。

【００４３】

ステップ１１２でレジスタ制御回路は、データ値内の各ビット位置に対して、その位置で書き込まれつつある現在のビットとその位置の、前に記憶されたビットとの排他的ＯＲの反転値を計算した後、この反転値とそのビット位置に対する前に記憶されたダミーレジスタ値との排他的ＯＲを計算する（図１１参照）。レジスタ制御回路１０２は、データレジスタにデータ値として書き込まれつつあるビットの反転値とともに、判定結果の反転値も計算する。これらの値は、書き込まれつつあるビットのすべて（たとえば、３個の３２ビットの値）に対して計算される。

【００４４】

ステップ１１４で、ステップ１０８と同様にデータレジスタにデータ値が書き込まれる。ステップ１１６で、当該レジスタの中の各ビット位置に対して判定された他の３個の値が他の３個のレジスタに書き込まれる。ステップ１１４とステップ１１６は同時に行われる。図１１に関連して説明するように、この結果、高から低への、低から高への遷移の数の平衡が取られるので、消費電力の平衡が取られる。

【００４５】
図１１はデータ書き込み動作の前後の可能なビット値の表を示す。データ値はレジスタＲｎに書き込まれつつあり、レジスタＲｎは対称書き込み動作機能が適用されているレジスタである。時点ｔおよび時点ｔ＋１における値が示されている。これらの値の反転値は簡単に判定される。この対称動作を受けるデータレジスタの各々に対して、専用のダミーレジスタ９８が設けられ、ダミーレジスタ９８はそのデータレジスタに現在保持されているデータ値の反転値を記憶する。
【００４６】
共用ダミーレジスタ１００は図１１ではレジスタＲｄとして示されている。共用ダミーレジスタＲｄ内の各ビット位置に対して、データ書き込みが行われるときにそのビット位置に書き込まれるべき新しい値は図１１の最下部に示されている関数によって決められる。この関数によって、データ値とデータ値の反転値に変化が生じないとき、変化は共用ダミーレジスタ内の対応するビットとその反転値で生じることが保証される。表は、データ値が変化しないときに生じる共用ダミーレジスタ内の変化と、データ値が変化するときに変化しない共用ダミーレジスタ内の共用値とを示す。このようにして、書き込み毎に一定数の遷移、すなわち、平衡の取れた等しい数の高から低への、低から高への遷移が保証される。
【００４７】
図１２は、書き込み動作がそれの条件コードに不合格となったときに書き込みを行うダミーデータレジスタＲＤの動作を示すフロー図である。ステップ１１８で、制御論理は命令の受信を待つ。制御論理は命令復号器６８であってもよいし、他の論理であってもよい。ステップ１２０で、命令がそれの条件コードに不合格であったか否かが判定される。命令がそれの条件コードに不合格でない場合には、その命令はステップ１２２で正規に実行され、その命令の中のレジスタオペランドによって指定されたレジスタへのそれの書き込みを行う。命令がそれの条件コードに不合格であった場合には、処理はステップ１２４に進み、ダミーデータレジスタ書き込みがイネーブルされるか否かについての判定が行われる。これらの書き込みがイネーブルされない場合には、処理は終了する。ダミーデータレジスタ書き込みがイネーブルされる場合には、処理はステップ１２６に進み、条件コードに不合格であっても、条件コードに不合格になった命令によって計算されたデータ値がトラッシュデータレジスタＲＴに書き込まれる。これにより、条件コードの合格、条件コードの不合格にかかわらず、電力消費とタイミングで平衡がとられる。トラッシュデータレジスタＲＴも、前に説明した遷移平衡機構の作用を受けることは理解されよう。
【００４８】
図１３は、少なくともいくつかの命令に対して多重命令実行機構が設けられるデータ処理システム１２８を示す。データ処理システム１２８は、少なくともいくつかのジャバのバイトコード命令のネイティブ実行をサポートするシステムである。この型のデータ処理システムとネイティブ実行については、発行されたＰＣＴ特許出願番号ＷＯ－Ａ－０２／２９５５５に説明されている。この発行された出願の全体としての、そして特にネイティブハードウェア実行とより複雑なジャバのバイトコードの選択的なソフトウェアエミュレーションについての開示は、ここに引用することにより本明細書の一部として組み入れられる。
【００４９】
ジャバのバイトコード復号器１３０は入力信号によって選択的にイネーブル、ディセーブルしてもよい。ジャバのバイトコード復号器１３０がディセーブルされたとき、受信されたジャバのバイトコードは例外をトリガし、この例外はネイティブＡＲＭサム（Ｔｈｕｍｂ）命令セットを使用してジャバのバイトコードを取り扱うためのソフトウェアエミュレーションコードの実行を開始する。図示するように、このサポートコードは領域１３２内のメモリ内に記憶される。ジャバのバイトコードのプログラム１３４もメモリ内に記憶される。ジャバのプログラムの実行の性質をおおい隠すことが望ましいとき、ジャバのバイトコード復号器１３０は擬似ランダム信号を受けてもよく、擬似ランダム信号はこの要

素を選択的にイネーブル、ディセーブルすることによりジャバのバイトコードに対する命令実行機構をハードウェアとエミュレーションの混合の実行機構と純粋なエミュレーション機構との間で効果的に切り換える。システム構成レジスタ１３６内の構成制御値は、ジャバ復号器１３０が存在するか否か、そしてこのジャバ復号器１３０のランダムなイネーブル、ディセーブルが許可されるか否かを指定する。図１４は受信されたジャバのバイトコードの取り扱いの概略図である。ステップ１３８で、ジャバのバイトコードが受信される。ステップ１４０で、ジャバ復号器１３０がイネーブルされているか判定される。ジャバ復号器１３０の擬似ランダムイネーブル、ディセーブルにより、ステップ１４２に分岐してバイトコードが常にエミュレーションされるか、またはステップ１４６でハードウェアで命令を実行する試みが効率的に行われる。これにより、ジャバのバイトコードの実行に関連付けられた電力シグネチャがおおい隠される／マスクされる。ステップ１４４での判定の結果、当該特定のジャバのバイトコードはジャバ復号器１３０によってサポートされず、このジャバのバイトコードはステップ１４２でソフトウェアでのエミュレーションも行われる。しかし、ジャバのバイトコードがハードウェアでサポートされる場合には、これはステップ１４６でハードウェアで実行される。

【図面の簡単な説明】

【００５０】

【図１】固定タイミングモードおよび可変タイミングモードで動作し得るデータ処理の概略図である。

【図２】条件付きプログラミング命令の概略図である。

【図３】本手法に従って動作する命令復号器によって遂行される処理動作の一部の概略を示すフロー図である。

【図４】固定タイミングモードでの条件付き分岐命令の実行の概略図である。

【図５】所要の処理動作またはダミー処理動作を遂行するように選択的にイネーブルされ得る多重回路部を含むデータ処理システムの概略図である。

【図６】所要のイネーブル信号とランダムダミーアクティビティイネーブル信号の両方に応答し得る回路部分とそれに関連付けられたダミーアクティビティイネーブル回路の概略図である。

【図７】擬似ランダム信号発生器として使用し得る線形シフト帰還レジスタの概略図である。

【図８】所要の処理アクティビティおよびダミー処理アクティビティを遂行するための回路部分の制御の概略を示すフロー図である。

【図９】条件付き書き込み動作がその条件付きコードに不合格となったときにダミーレジスタ書き込みが行われる多重データ処理レジスタ、多重ダミーレジスタ、多重共用ダミーレジスタ、および非マップトラッシュレジスタＲＴを含むレジスタバンクの一部の概略図である。

【図１０】レジスタ書き込みが行われるときに生じる高から低への、低から高への遷移の数を平衡させようとするレジスタ書き込み制御回路の概略を示すフロー図である。

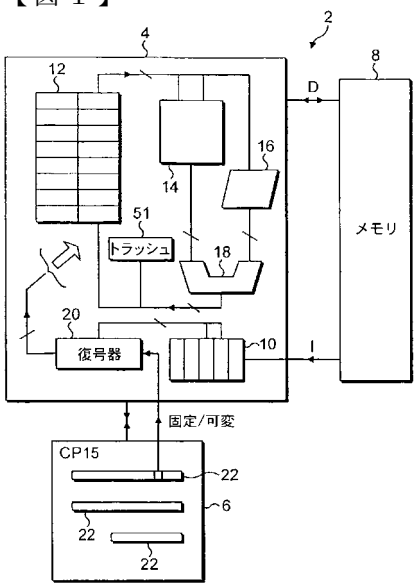
【図１１】レジスタ書き込みに伴って生じる高から低への、低から高への遷移を平衡させるように構成されるデータレジスタおよび他の３個のレジスタの中の特定のビットに対するビット遷移の間の関係を示す表である。

【図１２】書き込み動作の条件コードが不合格となったときに、トラッシュレジスタへの書き込みの制御の概略を示すフロー図である。

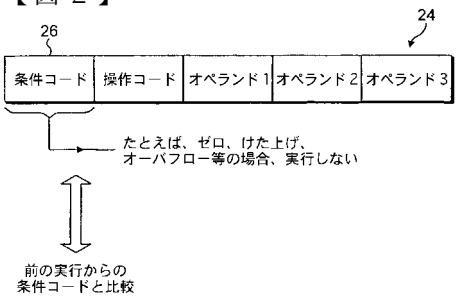
【図１３】一つの命令に対する多重実行機構をそなえるシステムと、少なくともいくつかの命令に対して用いられる実行機構の擬似ランダム選択の概略図である。

【図１４】図１３のシステムの制御の概略を示すフロー図である。

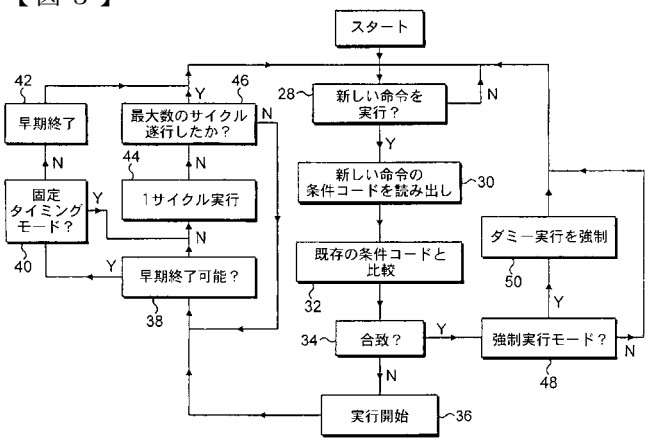
【図１】



【図２】

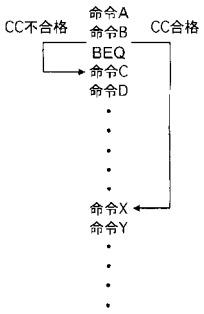


【図３】

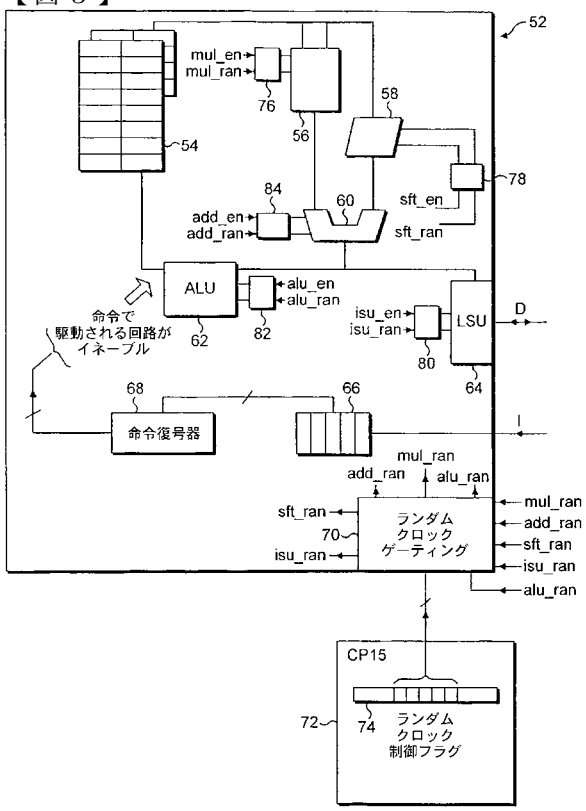


【図４】

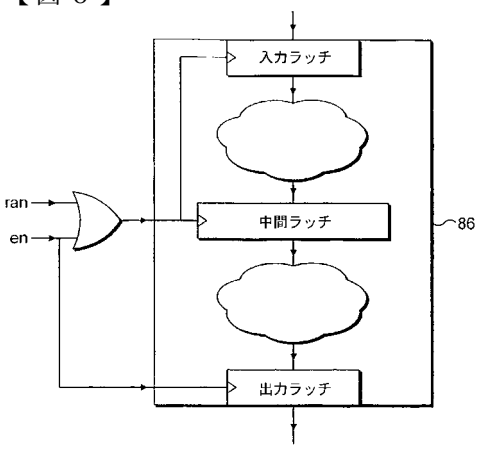
固定タイミングモードでの
条件付き分岐



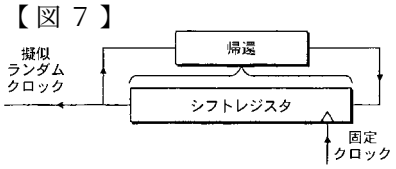
【図５】



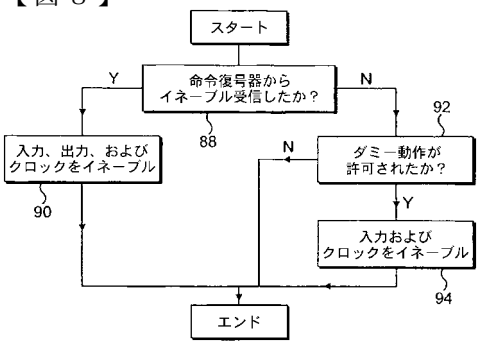
【図６】



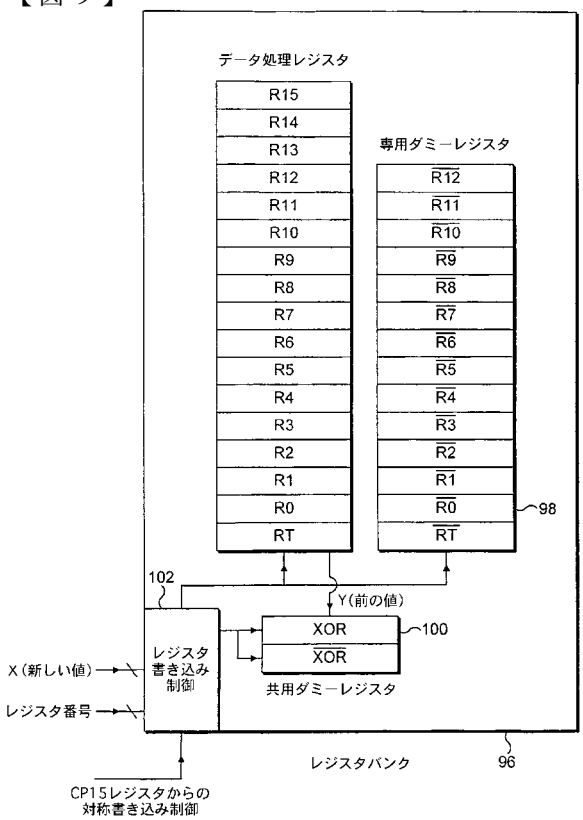
【図７】



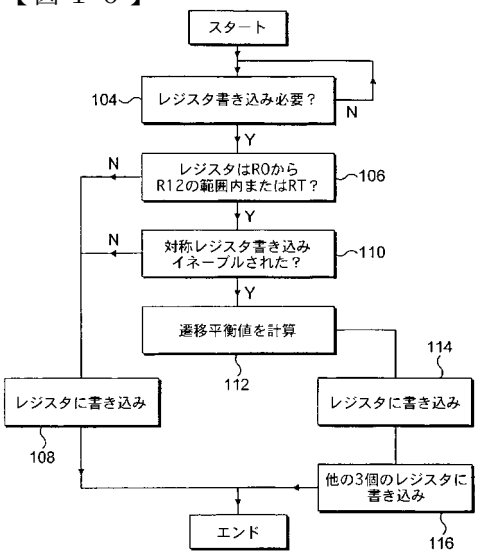
【図８】



【図９】



【図１０】

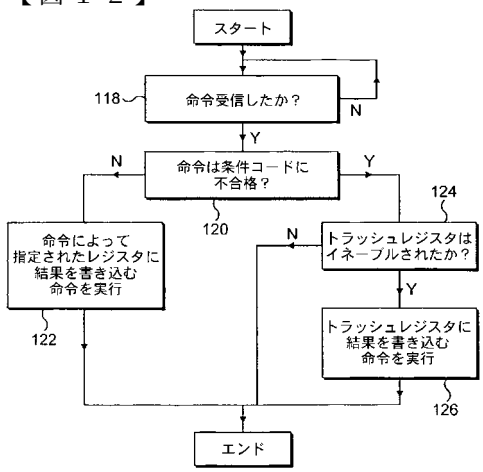


【図１１】

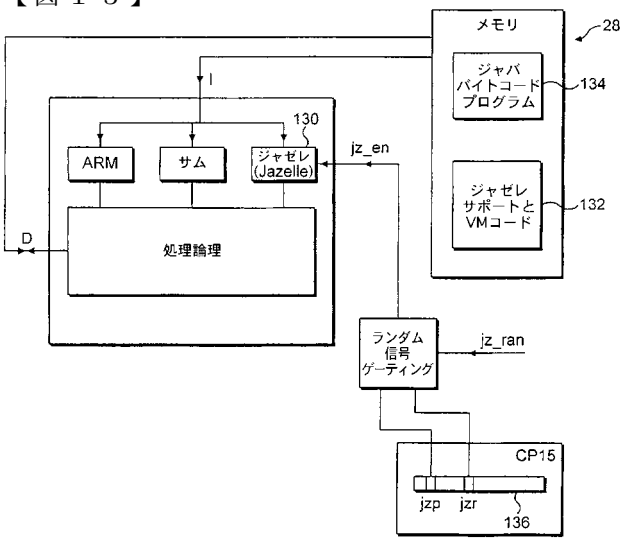
Rn[i]t	Rn[i]t+1	$\overline{Rn[i]t}$	$\overline{Rn[i]t+1}$	Rd[i]t	Rd[i]t+1	$\overline{Rd[i]t}$	$\overline{Rd[i]t+1}$	遷移 Rn	$\overline{Rn}$	Rd	$\overline{Rd}$
0	0	1	1	0	1	1	0	—	—	↑	↓
0	0	1	1	1	0	0	1	—	—	↓	↑
0	1	1	0	0	0	1	1	↑	↓	—	—
0	1	1	0	1	1	0	0	↑	↓	—	—
1	0	0	1	0	0	1	1	↓	↑	—	—
1	0	0	1	1	1	0	0	↓	↑	—	—
1	1	0	0	0	1	1	0	—	—	↑	↓
1	1	0	0	1	0	0	1	—	—	↓	↑

$$Rd[i]t+1 = \left(\overline{Rn[i]t \text{ XOR } Rn[i]t+1}\right) \text{ XOR } Rd[i]t$$

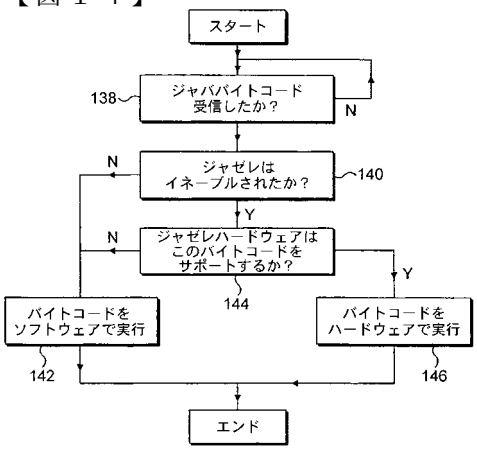
【図１２】



【図１３】



【図１４】



【手続補正書】
【提出日】平成16年10月13日(2004.10.13)
【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】
データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための装置であって、
データ処理命令の第一のセットを実行するように動作し得る第一の実行機構（１３０）と、
データ処理命令の第二のセットを実行するように動作し得る第二の実行機構であって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能であるように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、第二の実行機構と、
前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択するように動作し得る実行機構選択器（１４０）であって、擬似ランダム信号発生器によって発生される擬似ランダム実行機構選択信号（ｊ２－ｒａｎ）によって前記実行機構選択器が制御される、実行機構選択器と、
を具備するデータ処理装置。
【請求項２】
請求項１に記載された装置であって、前記第一の実行機構と前記第二の実行機構とは、

前記第一の実行機構または前記第二の実行機構によって実行可能である前記データ処理命令の少なくとも一つに対する少なくとも一つの異なる実行特性を備える、前記装置。
【請求項３】
請求項２に記載された装置であって、前記少なくとも一つの異なる実行特性は
前記データ処理命令を実行するための時間と、
前記データ処理命令を実行するときの電力消費
の一つ以上を含む、前記装置。
【請求項４】
請求項２と３のいずれか一つに記載された装置であって、前記第一の実行機構または前記第二の実行機構によって実行される少なくとも一つのデータ処理命令の少なくとも一つの実行特性が、先行するデータ処理命令が前記第一の実行機構または前記第二の実行機構で実行されたか否かに基づいて変動する、前記装置。
【請求項５】
先行する請求項のいずれか一つに記載された装置であって、前記データ処理命令のすべてが前記第一の実行機構または前記第二の実行機構によって実行可能である、前記装置。
【請求項６】
先行する請求項のいずれか一つに記載された装置であって、前記第一の実行機構は前記データ処理命令のいくつかを、データ処理ハードウェアを直接制御するネイティブ命令とエミュレーションソフトウェアを使用する残りのデータ処理命令として実行するように動作し得る、前記装置。
【請求項７】
先行する請求項のいずれか一つに記載された装置であって、前記第二の実行機構は、エミュレーションソフトウェアを使用する前記データ処理命令のすべてを実行するように動作し得る、前記装置。
【請求項８】
請求項６または７に記載された装置であって、前記第一の実行機構と前記第二の実行機構は少なくともいくつかのエミュレーションソフトウェアを共用する、前記装置。
【請求項９】
先行する請求項のいずれか一つに記載された装置であって、前記データ処理命令はジャバのバイトコード命令である、前記装置。
【請求項１０】
請求項９に記載された装置であって、前記第一の実行機構はネイティブのジャバのバイトコード実行ハードウェアを含み、前記第二の実行機構はすべてのジャバのバイトコードに対するジャバのバイトコードのエミュレーションを使用する、前記装置。
【請求項１１】
請求項１に記載された装置であって、プロセッサコアを具備し、前記擬似ランダム実行機構選択信号は前記プロセッサコアへの入力である、前記装置。
【請求項１２】
先行する請求項のいずれか一つに記載された装置であって、前記実行機構選択器にすべてのデータ処理命令に対して前記第一の実行機構を選択させるようにシステム構成バラメータが動作し得る、前記装置。
【請求項１３】
請求項１２に記載された装置であって、前記システム構成バラメータがシステム構成レジスタに記憶される、前記装置。
【請求項１４】
データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための方法であって、
第一の実行機構でデータ処理命令の第一のセットを実行するステップと、
第二の実行機構でデータ処理命令の第二のセットを実行することであって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能である

ように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、データ処理命令の第二のセットを実行するステップと、
前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、実行機構選択器で前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択するステップと、を含み、擬似ランダム信号発生器によって発生される擬似ランダム実行機構選択信号によって前記実行機構選択器を制御するようにしているデータ処理方法。
【請求項１５】
請求項１４に記載された方法であって、前記第一の実行機構と前記第二の実行機構とは、前記第一の実行機構または前記第二の実行機構によって実行可能である前記データ処理命令の少なくとも一つに対する少なくとも一つの異なる実行特性を備える、前記方法。
【請求項１６】
請求項１５に記載された方法であって、前記少なくとも一つの異なる実行特性は
前記データ処理命令を実行するための時間と、
前記データ処理命令を実行するときの電力消費
の一つ以上を含む、前記方法。
【請求項１７】
請求項１５と１６のいずれか一つに記載された方法であって、前記第一の実行機構または前記第二の実行機構によって実行される少なくとも一つのデータ処理命令の少なくとも一つの実行特性が、先行するデータ処理命令が前記第一の実行機構または前記第二の実行機構で実行されたか否かに基づいて変動する、前記方法。
【請求項１８】
請求項１４から１７のいずれか一つに記載された方法であって、前記データ処理命令のすべてが前記第一の実行機構または前記第二の実行機構によって実行可能である、前記方法。
【請求項１９】
請求項１４から１８のいずれか一つに記載された方法であって、前記第一の実行機構は前記データ処理命令のいくつかを、データ処理ハードウェアを直接制御するネイティブ命令とエミュレーションソフトウェアを使用する残りのデータ処理命令として実行するように動作し得る、前記方法。
【請求項２０】
請求項１４から１９のいずれか一つに記載された方法であって、前記第二の実行機構は、エミュレーションソフトウェアを使用する前記データ処理命令のすべてを実行するように動作し得る、前記方法。
【請求項２１】
請求項１９または２０に記載された方法であって、前記第一の実行機構と前記第二の実行機構は少なくともいくつかのエミュレーションソフトウェアを共用する、前記方法。
【請求項２２】
請求項１４から２１のいずれか一つに記載された方法であって、前記データ処理命令はジャバのバイトコード命令である、前記方法。
【請求項２３】
請求項２２に記載された方法であって、前記第一の実行機構はネイティブのジャバのバイトコード実行ハードウェアを含み、前記第二の実行機構はすべてのジャバのバイトコードに対するジャバのバイトコードのエミュレーションを使用する、前記方法。
【請求項２４】
請求項１４に記載された方法であって、プロセッサコアを具備し、前記擬似ランダム実行機構選択信号は前記プロセッサコアへの入力である、前記方法。
【請求項２５】
請求項１４から２４の請求項のいずれか一つに記載された方法であって、前記実行機構選択器にすべてのデータ処理命令に対して前記第一の実行機構を選択させるようにシステ

ム構成バラメータが動作し得る、前記方法。
【請求項２６】
請求項２５に記載された方法であって、前記システム構成バラメータがシステム構成レジスタに記憶される、前記方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００３
【補正方法】変更
【補正の内容】
【０００３】
このようなシステムの安全性を攻撃する知られている方法には、タイミング分析と電力分析が含まれる。入力に対するこのようなシステムのタイミング挙動（ｂｅｈａｖｉｏｕｒ）や電力消費挙動を観測することにより、遂行中の処理および操作中のデータに関する情報は、安全性を危うくし得る仕方で判定することができる。このような安全性攻撃に対する抵抗を設けることは非常に有益である。
ソング・エス・ピー他の「パワーＰＣ６０４ＲＩＳＣマイクロプロセッサ」、アイトリプルイーマイクロ（ＳＯＮＧ　Ｓ　Ｐ　ＥＴ　ＡＬ：“ＴＨＥ　ＰＯＷＥＲ　ＰＣ　６０４　ＲＩＳＣ　ＭＩＣＲＯＰＲＯＣＥＳＳＯＲ”　ＩＥＥＥ　ＭＩＣＲＯ，ＩＥＥＥ　ＩＮＣ．ＮＥＷ　ＹＯＲＫ，ＵＳ，ｖｏｌ．１４，ｎｏ．５，１　Ｏｃｔｏｂｅｒ　１９９４（１９９４－１０－０１）ｐａｇｅｓ８－１７，ＩＳＳＮ：０２７２－１７３２）には、アベラビリティに応じて、それに整数命令がディスパッチされ得る多重整数実行ユニットをそなえたプロセッサが開示されている。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００４
【補正方法】変更
【補正の内容】
【０００４】
一側面から見ると本発明は、データ処理動作を指定するデータ処理命令の制御下でデータの処理を行うための装置であって、
データ処理命令の第一のセットを実行するように動作し得る第一の実行機構と、
データ処理命令の第二のセットを実行するように動作し得る第二の実行機構であって、一つ以上のデータ処理命令が前記第一の実行機構または前記第二の実行機構によって実行可能であるように、前記データ処理命令の第一のセットが前記データ処理命令の第二のセットと部分的に重なる、第二の実行機構と、
前記第一の実行機構または前記第二の実行機構によって実行可能である一つ以上のデータ処理命令を実行するために、前記第一の実行機構または前記第二の実行機構を擬似ランダム的に選択するように動作し得る実行機構選択器であって、擬似ランダム信号発生器によって発生される擬似ランダム実行機構選択信号によって前記実行機構選択器が制御される、実行機構選択器と
を具備するデータ処理のための装置を提供する。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Ir ional Application No
PCT/GB 03/04313

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SONG S P ET AL: "THE POWER PC 604 RISC MICROPROCESSOR" IEEE MICRO, IEEE INC. NEW YORK, US, vol. 14, no. 5, 1 October 1994 (1994-10-01), pages 8-17, XP000476676 ISSN: 0272-1732 page 8, left-hand column, paragraph 2 - right-hand column, last paragraph page 13; figure 4 page 12, left-hand column, paragraph 3 - right-hand column, last paragraph	1-3,5, 11,12, 16-18, 20,26,27
A	WO 00/39660 A (UGON MICHEL ; BULL CP8 (FR); GRESSUS YVON (FR); SIEGELIN CHRISTOPH (FR) 6 July 2000 (2000-07-06) the whole document	1
	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

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

Date of the actual completion of the international search	Date of mailing of the international search report
2 June 2004	14/06/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Alecu, M

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 03/04313

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/066003 A1 (ROSE ANDREW CHRISTOPHER ET AL) 30 May 2002 (2002-05-30) column 2, paragraph 9 - paragraph 10 column 12, paragraph 86	1-30
A	US 6 298 434 B1 (LINDWER MENNO M) 2 October 2001 (2001-10-02) the whole document	1-30
A	US 6 332 215 B1 (RANGANATH V R ET AL) 18 December 2001 (2001-12-18) the whole document	1-30

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 03/04313

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0039660 A	06-07-2000	FR 2787900 A1	30-06-2000
		BR 9908268 A	24-10-2000
		CN 1124533 B	15-10-2003
		EP 1057094 A1	06-12-2000
		WO 0039660 A1	06-07-2000
		JP 2002533825 T	08-10-2002
		TW 463101 B	11-11-2001
US 2002066003 A1	30-05-2002	GB 2367653 A	10-04-2002
		CN 1434938 T	06-08-2003
		EP 1323032 A1	02-07-2003
		GB 2367658 A	10-04-2002
		WO 0229555 A1	11-04-2002
		JP 2002116908 A	19-04-2002
		JP 2004511041 T	08-04-2004
		US 2002069402 A1	06-06-2002
		US 2002108103 A1	08-08-2002
US 6298434 B1	02-10-2001	DE 69820027 D1	08-01-2004
		EP 1359501 A2	05-11-2003
		EP 0950216 A2	20-10-1999
		EP 0941508 A1	15-09-1999
		EP 1019794 A2	19-07-2000
		WO 9918484 A2	15-04-1999
		WO 9918485 A2	15-04-1999
		WO 9918486 A2	15-04-1999
		JP 2001508907 T	03-07-2001
		JP 2001508908 T	03-07-2001
		JP 2001508909 T	03-07-2001
		US 2002129225 A1	12-09-2002
		US 6292883 B1	18-09-2001
		US 6349377 B1	19-02-2002
US 6332215 B1	18-12-2001	AU 2165400 A	26-06-2000
		EP 1157323 A2	28-11-2001
		JP 2002532772 T	02-10-2002
		WO 0034844 A2	15-06-2000
		US 6338160 B1	08-01-2002
		US 2002019976 A1	14-02-2002
		US 2002066083 A1	30-05-2002

フロントページの続き

(31)優先権主張番号 0307823.5
(32)優先日 平成15年4月4日(2003.4.4)
(33)優先権主張国 英国(GB)

(81)指定国 GB,JP,US

(72)発明者 ピリー、フレデリック、クロード、マリー
フランス国、カーニュ シュル メール、 シェマン デ プラト フルーリ、１１

Ｆターム(参考) 5B033 BA02 BA03 FA27
5B076 FC08 FC09 FD04 FD07
5B276 FC08 FC09 FD04 FD07