【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17年7月14日(2005.7.14)

【公開番号】特開2002-258743(P2002-258743A)
【公開日】平成14年9月11日(2002.9.11)
【出願番号】特願2001-60223(P2001-60223)
【国際特許分類第７版】
　Ｇ０９Ｃ　1/00
　Ｇ０６Ｆ　7/72
　Ｇ０６Ｆ　12/14
　Ｇ０６Ｋ　19/07
　Ｈ０４Ｌ　9/10
【ＦＩ】
　Ｇ０９Ｃ　1/00　６２０Ｂ
　Ｇ０９Ｃ　1/00　６２０Ｚ
　Ｇ０９Ｃ　1/00　６６０Ａ
　Ｇ０６Ｆ　7/72
　Ｇ０６Ｆ　12/14　３２０Ｂ
　Ｇ０６Ｋ　19/00　Ｎ
　Ｈ０４Ｌ　9/00　６２１Ｚ

【手続補正書】
【提出日】平成16年11月19日(2004.11.19)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　外部とのデータ送受信を行う入出力ポートと、プログラムとデータを格納する記憶装置と、前記プログラムに従ってデータ処理を実行する演算装置と、前記入出力ポート、記憶装置および演算装置を接続するバスとを有する情報処理装置における、データ処理と消費電流との関連性を減らすための方法であって、前記データ処理に関して、前記演算装置が暗号処理中に出現する剰余乗算であるＡ＊Ｂ＊Ｒ＾（－１）　ｍｏｄ　Ｎを計算する際に実行されるその方法は、
（１）次のステップ（２）と（３）のいずれかをランダムに選択するステップ、
（２）モンゴメリ法に従ってビットストリングデータについてS_1＝Ａ＊Ｂ＊Ｒ＾（－１）　ｍｏｄ　Ｎ（Ｂは乗数、Ａは被乗数、Ｎは２つの大きな素数の積、Ｒは２＾（前記ビットストリングデータのビット長））を計算するステップ、
（３）S_2＝｛ｓＮ＋Ａ*(-1)^ｆ｝＊｛ｔＮ＋Ｂ*(-1)^ｇ｝　Ｒ＾（－１）　ｍｏｄ　Ｎ（任意の整数ｓ，ｔ，ｆ，ｇは少なくとも１つは０でない整数であり、ｆ，ｇは０又は１）を計算するステップ、
（４）前記ビットストリングデータを構成する各々のビットブロックについて上記（１）（２）（３）を繰り返し、最後に前記ビットストリングデータの最後のビットブロックについて上記（２）を選択したときには計算結果S_1についてT_1＝S_1＊Ｒ＾（－１）ｍｏｄＮを計算してT_1を出力し、上記（３）を選択したときには計算結果S_2についてT_2＝S_2＊Ｒ＾（－１）　ｍｏｄＮを計算してＮ－T_2を出力するステップ、および
（５）T_1とＮ－T_2を、暗号処理の剰余乗算Ａ＊Ｂ＊Ｒ＾（－１）　ｍｏｄ　Ｎの計算結

果として用いるステップを有することを特徴とする耐タンパーモジュラ演算処理方法。
【請求項２】
前記（１）の選択するとは、乱数を用いていずれかを選択することを特徴とする請求項１記載の耐タンパーモジュラ演算処理方法。
【請求項３】
前記（ｓ，ｔ，ｆ，ｇ）は、(０，１，０，１)であることを特徴とする請求項１記載の耐タンパーモジュラ演算処理方法。
【請求項４】
前記（ｓ，ｔ，ｆ，ｇ）は、(１，０，１，０)であることを特徴とする請求項１記載の耐タンパーモジュラ演算処理方法。
【請求項５】
外部とのデータ送受信を行う入出力ポートと、プログラムとデータを格納する記憶装置と、前記プログラムに従ってデータ処理を実行する演算装置と、前記入出力ポート、記憶装置および演算装置を接続するバスとを有する情報処理装置における、データ処理と消費電流との関連性を減らすための方法であって、前記データ処理に関して、前記演算装置が暗号処理中に出現する剰余乗算であるＡ＊Ｂ ｍｏｄ ｐ （ｐは素数）を計算する際に実行されるその方法は、
（１）次のステップ（２）と（３）のいずれかをランダムに選択するステップ、
（２）ビットストリングデータについてＳ＝Ａ＊Ｂ ｍｏｄ ｐ（Ｂは乗数、Ａは被乗数）を計算するステップ、
（３）Ｓ＝｛ｓｐ ＋ Ａ*(-1)^ｆ｝＊｛ｔｐ ＋ Ｂ*(-1)^ｇ｝ ｍｏｄ ｐ （任意の整数ｓ，ｔ，ｆ，ｇは少なくとも１つは０でない整数であり、ｆ，ｇは０又は１でｆ＋ｇは偶数）を計算するステップ、および
（４）上記（２）と（３）のうち選択された方の計算結果Ｓを暗号処理の剰余乗算Ａ＊Ｂ ｍｏｄ ｐの計算結果として用いるステップを有することを特徴とする耐タンパーモジュラ演算処理方法。
【請求項６】
前記（ｓ，ｔ，ｆ，ｇ）は、(１，１，１，１)であることを特徴とする請求項５記載の耐タンパーモジュラ演算処理方法。
【請求項７】
前記（３）のステップのｆ＋ｇは奇数であって、前記（４）の代わりに、
（４）前記（２）を選択したときは計算結果Ｓそのままとし、前記（３）を選択したときにはＳの代わりにｐ－Ｓを計算結果とするステップ、および
（５）前記Ｓとｐ－Ｓを、暗号処理の剰余乗算Ａ＊Ｂ ｍｏｄ ｐの計算結果として用いるステップを有することを特徴とする請求項５記載の耐タンパーモジュラ演算処理方法。
【請求項８】
前記（ｓ，ｔ，ｆ，ｇ）は、(０，１，０，１)であることを特徴とする請求項７記載の耐タンパーモジュラ演算処理方法。
【請求項９】
外部とのデータ送受信を行う入出力ポートと、プログラムとデータを格納する記憶装置と、前記プログラムに従ってデータ処理を実行する演算装置と、前記入出力ポート、記憶装置および演算装置を接続するバスとを有する情報処理装置における、データ処理と消費電流との関連性を減らすための方法であって、前記データ処理に関して、前記演算装置が暗号処理中に出現する剰余乗算であるＡ（ｘ）＊Ｂ（ｘ） ｍｏｄ Φ（ｘ）（Φ（ｘ）はｘの既約多項式であり、Ａ（ｘ）＊Ｂ（ｘ）の係数の演算は３以上の素数ｐを法として行う）を計算する際に実行されるその方法は、
（１）次のステップ（２）と（３）のいずれかをランダムに選択するステップ、
（２）Ｓ（ｘ）＝Ａ（ｘ）＊Ｂ（ｘ） ｍｏｄ Φ（ｘ）（Ａ（ｘ）又はＢ（ｘ）はｘの多項式）を計算するステップ、
（３）Ｓ（ｘ）＝｛ｓΦ（ｘ） ＋ Ａ（ｘ）*(-1)^ｆ｝＊｛ｔΦ（ｘ） ＋ Ｂ（ｘ）*(-1)

^g} ｍｏｄ Φ（ｘ）（任意の整数ｓ，ｔ，ｆ，ｇは少なくとも１つは０でない整数であり、ｆ，ｇは０又は１でｆ＋ｇは偶数）を計算するステップ、および
（４）上記（２）と（３）のうち選択された方の計算結果Ｓ（ｘ）を、暗号処理の剰余乗算Ａ（ｘ）＊Ｂ（ｘ） ｍｏｄ Φ（ｘ）の計算結果として用いるステップを有することを特徴とする耐タンパーモジュラ演算処理方法。

【請求項１０】
前記（ｓ，ｔ，ｆ，ｇ）は、(１，１，１，１)であることを特徴とする請求項９記載の耐タンパーモジュラ演算処理方法。

【請求項１１】
前記（３）のステップのｆ＋ｇは奇数であって、前記（４）の代わりに、
（４）前記（２）を選択したときは計算結果Ｓ（ｘ）そのままとし、上記（３）を選択したときにはＳ（ｘ）の代わりにΦ（ｘ）－Ｓ（ｘ）を計算結果とするステップ、および
（５）前記Ｓ（ｘ）とΦ（ｘ）－Ｓ（ｘ）を、暗号処理の剰余乗算Ａ（ｘ）＊Ｂ（ｘ）ｍｏｄ Φ（ｘ）の計算結果として用いるステップを有することを特徴とする請求項９記載の耐タンパーモジュラ演算処理方法。

【請求項１２】
前記（ｓ，ｔ，ｆ，ｇ）は、(０，１，０，１)であることを特徴とする請求項１１記載の耐タンパーモジュラ演算処理方法。

【請求項１３】
前記Ａ（ｘ）＊Ｂ（ｘ）の係数の演算は素数２を法として行うものであり、前記（３）の（ｆ，ｇ）は（０，０）であることを特徴とする請求項９記載の耐タンパーモジュラ演算処理方法。