(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-242573
(P2012-242573A)
(43)公開日　平成24年12月10日(2012.12.10)

(51)Int.Cl.			F I			テーマコード（参考）
G09C	1/00	(2006.01)	G09C	1/00	620B	5J104
H04L	9/10	(2006.01)	H04L	9/00	621A	

審査請求 未請求　請求項の数 3　ＯＬ　（全 14 頁）

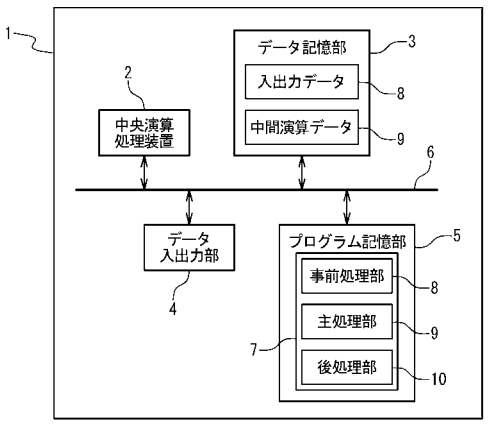
(21)出願番号　特願2011-112058 (P2011-112058)
(22)出願日　平成23年5月19日 (2011.5.19)

(71)出願人　302062931
ルネサスエレクトロニクス株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100102864
弁理士　工藤　実
(72)発明者　東　邦彦
神奈川県横浜市神奈川区金港町３番地１
ルネサスマイクロシステム株式会社内

Ｆターム(参考)　5J104 AA16　AA22　AA46　AA47　JA21
JA28　NA02　NA18　NA37

(54)【発明の名称】復号処理装置、復号処理方法、及び復号処理プログラム

(57)【要約】　（修正有）
【課題】ＲＳＡ暗号の高速な復号のために、ＣＲＴ（中国人剰余定理）と呼ばれる高速演算アルゴリズムを適用し、電力差分解析攻撃に対する耐性を高めつつ、中間演算データによるメモリ消費量を削減できる、復号処理装置、復号処理方法、及び復号処理プログラムを提供する。
【解決手段】ＣＲＴが適用されるＲＳＡ復号処理の後処理において、計算式「Ｚ＝Ｃ×ｑ＋Ｃｑ」の代わりに、ｒをｐ及びｑよりも大きい奇数である秘密変数として、計算式「Ｚ＝（Ｃ×ｑ（ｒ＋１）＋Ｃｑ）ｍｏｄｑｒ」を用いる。
【選択図】図５



【特許請求の範囲】
【請求項１】
メッセージＭを示すメッセージデータ、秘密素数ｐを示すｐデータ、秘密素数ｑを示すｑデータ、秘密鍵ｄを示すｄデータ、及び、前記ｐ及び前記ｑよりも大きい奇数である秘密変数ｒを示す秘密変数データを格納する、データ記憶部と、
事前処理部と、
主処理部と、
後処理部と、
を具備し、
前記メッセージＭは、平文Ｚ、公開鍵ｅ、及び公開鍵Ｎに基づいて、下記式１により得られたものであり、
（数式１）：$M = Z^{e} \bmod N$
前記ｅは、（ｐ－１）×（ｑ－１）と互いに素である正の整数であり、
前記Ｎは、ｐ×ｑにより表される数であり、
前記ｄは、（ｐ－１）×（ｑ－１）を法とした前記ｅの逆元を示す数であり、
前記事前処理部は、前記ｐデータ、前記ｑデータ、及び前記ｄデータに基づいて、下記式２乃至４によって表される計算を行い、ｕを示すｕデータ、d_pを示すd_pデータ、及びd_qを示すd_qデータを生成し、
（数式２）：$u = q^{-1} \bmod p$
（数式３）：$d_p = d \bmod (p-1)$
（数式４）：$d_q = d \bmod (q-1)$
前記主処理部は、前記メッセージＭ、前記ｐデータ、及び前記ｑデータに基づいて、下記式５及び６によって表される計算を行い、M_pを示すM_pデータ、及びM_qを示すM_qデータを生成し、前記M_pデータ、前記d_pデータ、前記ｐデータ、前記M_qデータ、前記d_qデータ、及び前記ｑデータに基づいて、下記式７及び８によって表される計算を行い、Ｃｐを示すＣｐデータ及びＣｑを示すＣｑデータを生成し、
（数式５）：$M_p = M \bmod p$
（数式６）：$M_q = M \bmod q$
（数式７）：$Cp = (M_p)^{d_p} \bmod p$
（数式８）：$Cq = (M_q)^{d_q} \bmod q$
前記後処理部は、前記Ｃｐデータ、前記Ｃｑデータ、前記ｕデータ、及び前記ｐデータに基づいて、下記式９によって表される計算を行い、Ｃを示すＣデータを生成し、前記Ｃデータ、前記ｑデータ、前記ｒデータ、前記Ｃｑデータに基づいて、下記式１０又は１１によって表される計算を行い、前記平文Ｚを示す出力データを生成し、
（数式９）：$C = ((C_p - C_q) \times u) \bmod p$
（数式１０）；$Z = (C \times q(r+1) + C_q) \bmod qr$
（数式１１）；$Z = (C \times q(k \times r + 1) + C_q) \bmod qr$
上式１１中、ｋは任意の定数を示す
復号処理装置。
【請求項２】
コンピュータが、メッセージＭを示すメッセージデータ、秘密素数ｐを示すｐデータ、秘密素数ｑを示すｑデータ、秘密鍵であるｄを示すｄデータ、及び、前記ｐ及び前記ｑよりも大きい奇数である秘密変数ｒを示す秘密変数データを取得するステップと、
コンピュータが、事前処理を行うステップと、
コンピュータが、主処理を行うステップと、
コンピュータが、後処理を行うステップと、
を具備し、
前記メッセージＭは、平文Ｚ、公開鍵ｅ、及び公開鍵Ｎに基づいて、下記式１により得られたものであり、
（数式１）：$M = Z^{e} \bmod N$

前記ｅは、（ｐ－１）×（ｑ－１）と互いに素である整数であり、
前記Ｎは、ｐ×ｑにより表される数であり、
前記ｄは、（ｐ－１）×（ｑ－１）を法とした前記ｅの逆元を示す数であり、
前記事前処理を行うステップは、前記ｐデータ、前記ｑデータ、及び前記ｄデータに基づいて、下記式２乃至４によって表される計算を行い、ｕを示すｕデータ、d_pを示すd_pデータ、及びd_qを示すd_qデータを生成するステップを含み、
（数式２）：$u = q^{-1} \bmod p$
（数式３）：$d_p = d \bmod (p-1)$
（数式４）：$d_q = d \bmod (q-1)$
前記主処理を行うステップは、前記メッセージＭ、前記ｐデータ、及び前記ｑデータに基づいて、下記式５及び６によって表される計算を行い、Ｍｐを示すＭｐデータ、及びＭｑを示すＭｑデータを生成し、前記M_pデータ、前記d_pデータ、前記ｐデータ、前記M_qデータ、前記d_qデータ、及び前記ｑデータに基づいて、下記式７及び８によって表される計算を行い、Ｃｐを示すＣｐデータ及びＣｑを示すＣｑデータを生成ステップを含み、
（数式５）：$M_p = M \bmod p$
（数式６）：$M_q = M \bmod q$
（数式７）：$Cp = (M_p)^{d_p} \bmod p$
（数式８）：$Cq = (M_q)^{d_q} \bmod q$
前記後処理を行うステップは、前記ＣｐデータＣｑデータ、前記ｕデータ、及び前記ｐデータに基づいて、下記式９によって表される計算を行い、Ｃを示すＣデータを生成し、前記Ｃデータ、前記ｑデータ、前記ｒデータ、前記ＣｑデータＣｑデータに基づいて、下記式１０又は１１によって表される計算を行い、前記平文Ｚを示す出力データを生成するステップを含み、
（数式９）：$C = ((C_p - C_q) \times u) \bmod p$
（数式１０）；$Z = (C \times q(r+1) + C_q) \bmod qr$
（数式１１）；$Z = (C \times q(k \times r + 1) + C_q) \bmod qr$
上式１１中、ｋは任意の定数を示す
復号処理方法。
【請求項３】
請求項２に記載される復号処理方法をコンピュータにより実現するための復号処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、復号処理装置、復号処理方法、及び復号処理プログラムに関する。
【背景技術】
【０００２】
昨今、ユビキタスネットワーク社会において、復号処理が様々な情報機器に利用されている。復号処理の方式として、公開鍵暗号方式が知られている。代表的な公開鍵暗号方式として、ＲＳＡ暗号方式が知られている。ＲＳＡ暗号方式では、べき乗剰余演算が行われる。べき乗剰余演算は、コンピュータにより、実行される。以下に、ＲＳＡ暗号方式について説明する。
【０００３】
ＲＳＡ暗号方式では、秘密素数ｐ、秘密素数ｑ、公開鍵ｅ、公開鍵Ｎ、及び秘密鍵ｄが用いられる。ここで、公開鍵Ｎは、式「Ｎ＝ｐ×ｑ」により、与えられる。また、公開鍵ｅは、（ｐ－１）×（ｑ－１）と互いに素である正の整数である。秘密鍵ｄは、（ｐ－１）×（ｑ－１）を法とした公開鍵ｅの逆元である。
【０００４】
平文Ｚを暗号文Ｍ（メッセージＭ）に変換する場合には、公開鍵ｅ及び公開鍵Ｎを用い

て、下記式１により示される計算が行なわれる。
（数式１）：Ｍ＝Ｚ^{e}ｍｏｄＮ
一方、メッセージＭを平文Ｚに変換（復号）する場合には、秘密鍵ｄ及び公開鍵Ｎを用いて、下記式２により示される計算が行なわれる。
（数式２）：Ｚ＝Ｍ^{d}ｍｏｄＮ
尚、「ＡｍｏｄＢ」とは、Ｂを法としたＡの剰余を示す。
【０００５】
上述のように、復号時（数式２の演算時）には、Ｍ、ｄ、及びＮを用いて、べき乗剰余演算が実行される。ここで、第三者による解読を困難にするために、Ｍ、ｄ、及びＮとして、非常に大きな数値（例えばそれぞれ１０２４ｂｉｔなど）が用いられる。しかしながら、これによって、復号時においてべき乗剰余演算に費やされる処理時間が、長くなってしまう。
【０００６】
べき乗剰余演算に要する処理時間を短縮するために、一般的には、中国人剰余定理（Ｃｈｉｎｅｓｅ　Ｒｅｍａｉｎｄｅｒ　Ｔｈｅｏｒｅｍ：以降ＣＲＴと称す）と呼ばれる高速演算アルゴリズムが適用される。ＣＲＴを用いることにより、べき乗剰余演算に費やされる処理時間を１／４に短縮できることが知られている。
【０００７】
以下に、ＣＲＴが適用されるＲＳＡ復号処理について説明する。図１は、ＣＲＴを適用した復号処理を示すフローチャートである。図１に示されるように、事前処理として、秘密鍵ｐ、ｑ、ｕ、ｄｐ、及びｄｑを示すデータが、コンピュータに入力される（ステップＳ１０１）。ここで、ｕ，ｄｐ，及びｄｑは、下記式３乃至５によって表される式により求められた値である。
（数式３）：ｕ＝（１／ｑ）ｍｏｄｐ
（数式４）：ｄｐ＝ｄｍｏｄ（ｐ－１）
（数式５）：ｄｑ＝ｄｍｏｄ（ｑ－１）
【０００８】
次いで、メッセージＭを示すデータがコンピュータに入力される（ステップＳ１０２）。
【０００９】
次いで、コンピュータが、主処理が行う。主処理として、下記式６及び７に従って、Ｍｐ及びＭｑが求められる（ステップＳ１０３）。また、下記式８及び９に従って、Ｃｐ及びＣｑが求められる（ステップＳ１０４）。
（数式６）：Ｍｐ＝Ｍｍｏｄｐ
（数式７）：Ｍｑ＝Ｍｍｏｄｑ
（数式８）：Ｃｐ＝Ｍｐ^{dp}ｍｏｄｐ
（数式９）：Ｃｑ＝Ｍｑ^{dq}ｍｏｄｑ
【００１０】
次いで、コンピュータが、後処理を行なう。後処理として、下記式１０及び１１に従って、Ｃ及び平文Ｚが求められる（ステップＳ１０５）。
（数式１０）：Ｃ＝（（Ｃｐ－Ｃｑ）×ｕ）ｍｏｄｐ
（数式１１）：Ｚ＝Ｃ×ｑ＋Ｃｑ
【００１１】
そして、数式１１により求められた平文Ｚが、復号結果として出力される（ステップＳ１０６）。すなわち、ＣＲＴを用いた場合には、数式２によって示される演算が、数式３乃至１１を用いることにより、実行される。
【００１２】
一方で、暗号処理方式の脆弱性を研究及び開発する活動が、盛んに行なわれている。特に、サイドチャネル攻撃と呼ばれる攻撃手法の研究が、学会等を賑やかせている。サイドチャネル攻撃の一手法として、電力差分解析攻撃（ＤＰＡ：Ｄｉｆｆｅｒｅｎｔｉａｌ

Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ）という手法が存在する。デバイスの消費電力は、実行されている演算、及び用いられているデータ値に関係する場合がある。電力差分解析攻撃では、この点が利用される。すなわち、復号処理を行っている時の消費電力が測定され、統計処理が行われ、復号処理内容に関する情報（秘密鍵などの機密情報）が導出される。

【００１３】

ＣＲＴが適用されたＲＳＡ暗号処理方式においては、電力差分解析攻撃に対して非常に脆弱な処理部分が存在する。非特許文献１（Ｐａｐｅｒ　ｏｎ　ＤＰＡ　ｒｅｃｏｍｂｉｎａｔｉｏｎ　ａｔｔａｃｋ　ｏｎ　ＲＳＡ－ＣＲＴ、ｈｔｔｐ：／／ｗｗｗ．ｒｉｓｃｕｒｅ．ｃｏｍ／ｔｅｃｈ－ｃｏｒｎｅｒ／ｐｕｂｌｉｃａｔｉｏｎｓ．ｈｔｍｌ）には、再結合処理（Ｒｅｃｏｍｂｉｎａｔｉｏｎ）と呼ばれる処理（数式１０及び数式１１）が、電力差分解析攻撃に対する脆弱性を有している点が開示されている。

【００１４】

一方、特許文献１（特開２００６－２１７１９３号公報）には、再結合処理に対する電力差分解析攻撃を用いたアタックを困難にするための復号処理方法が、開示されている。

【００１５】

図２Ａは、特許文献１に記載された復号処理方法を示すフローチャートである。また、図３は、特許文献１に記載された復号処理方法において、記憶装置に格納されるデータを示す構成図である。図２Ａに示されるように、この復号処理方法では、ステップＳ１００において、入力データであるメッセージＭが外部から受信される。メッセージＭは、記憶装置における一時データ格納部（図３参照）に格納される。次いで、ステップＳ１０１において、記憶装置における永続データ格納部（図３参照）に格納に格納された秘密鍵（ｐ，ｑ，ｕ，ｄｐ，ｄｑ）を用いて、メッセージＭに対するＲＳＡ計算が実行され、出力データである平文Ｚが計算される。平文Ｚは、一時データ格納部に格納される。ステップＳ１０２において、平文Ｚが外部に送信される。

【００１６】

図２Ｂは、上述のステップＳ１０２における処理を詳細に示すフローチャートである。

【００１７】

図２Ｂに示されるように、ステップＳ１１１において、Ｍのｐを法とした剰余Ｍｐ、及びＭのｑを法とした剰余Ｍｑが計算され、計算結果が一時データ格納部に格納される。また、ｄｐを指数かつｐを法としたＭｐのべき乗剰余Ｃｐ、及び、ｄｐを指数かつｑを法としたＭｑのべき乗剰余Ｃｑが計算され、計算結果が一時データ格納部に格納される。

【００１８】

次に、ステップＳ１１２において、乱数ｒ１が生成され、一時データ格納部２３３に格納される。次に、ステップＳ１１３において、ｒ１の値が、ｕを法とするｒ１の剰余ｒ１を計算することにより、更新される。次に、ステップＳ１１４において、ｕからｒ１を減算することにより、ｒ２が計算される。ｒ２を示すデータは、データ格納部に格納される。次に、ステップＳ１１５にて、ｐを法としたＣｐ－Ｃｑの剰余Ｃ０が計算され、データ格納部に格納される。次にＳ１１６において、ｐを法としたＣ０とｒ１の乗算剰余Ｃ１と、Ｃ０とｒ２の乗算剰余Ｃ２とが計算され、一時データ格納部に格納される。次に、ステップＳ１１７において、Ｃ１とｑの乗算Ｚ１と、Ｃ２とｑの乗算Ｚ２とが計算され、一時データ格納部に格納される。次に、ステップＳ１１８において、ｐとｑの乗算Ｎが計算され、一時データ格納部に格納される。次に、ステップＳ１１９において、Ｎを法としたＺ１とＺ２の加算剰余に、Ｃｑが加算され、Ｚとして、一時データ格納部に格納される。

【００１９】

特許文献１の記載によれば、ステップＳ１１２乃至Ｓ１１４において、乱数ｒ１及びｒ２が生成される。そして、ステップＳ１１６において、これらの乱数ｒ１及びｒ２を用いて、Ｃの値が、Ｃ１及びＣ２にランダムに分解される。そして、Ｃとｑの乗算を計算する代わりに、ステップＳ１１７において、Ｃ１とｑの乗算Ｚ１、及び、Ｃ２とｑの乗算Ｚ２が計算される。最後に、ステップＳ１１９において、Ｚ１とＺ２とが加算され、Ｃとｑとの乗算が実現される。ここで、乱数ｒ１とｒ２の値は、ＲＳＡ計算を行う度に異なった値

になる。Ｃとｑとの乗算を行う際に、毎回異なる乱数値が用いられるため、Ｃとｑとを乗算する際における消費電力を繰り返し観察したとしても、ｑの値を推測することが困難になる。

【先行技術文献】

【特許文献】

【００２０】

【特許文献１】特開２００６－２１７１９３号公報

【非特許文献】

【００２１】

【非特許文献１】Ｐａｐｅｒ ｏｎ ＤＰＡ ｒｅｃｏｍｂｉｎａｔｉｏｎ ａｔｔａｃｋ ｏｎ ＲＳＡ－ＣＲＴ、 ｈｔｔｐ：／／ｗｗｗ．ｒｉｓｃｕｒｅ．ｃｏｍ／ｔｅｃｈ－ｃｏｒｎｅｒ／ｐｕｂｌｉｃａｔｉｏｎｓ．ｈｔｍｌ

【発明の概要】

【発明が解決しようとする課題】

【００２２】

特許文献１に記載された方法によれば、電力差分解析攻撃に対する耐性を高めることができる。しかしながら、この方法では、剰余加減算や剰余乗算を処理可能なコプロセッサを用いた場合であっても、図３に示したように大量の中間演算データが発生する。そのようなコプロセッサを搭載していないコンピュータ（通常のコンピュータ）を用いる場合には、更に大量の中間演算データが発生する。図４は、特許文献１に記載された方法が通常のコンピュータによって実行される場合に発生する中間演算データを示す概略図である。図４には、鍵長が１０２４ｂｉｔである場合の例が示されている。図４に示される例では、入力データとして、それぞれ５１２ｂｉｔであるｐ、ｑ、ｄ、及び、１０２４ｂｉｔであるメッセージＭが用いられている。図４に示されるように、中間演算データとして、１４個（ｕ，ｄｐ，ｄｑ，Ｍｐ，Ｍｑ，Ｃｐ，Ｃｑ，ｒ１，ｒ３，ｒ２，Ｃ００，Ｃ０，Ｃ１，及びＣ２）の５１２ｂｉｔのデータが発生し、８個（Ｃ１１，Ｃ２１、Ｚ１、Ｚ２、Ｎ、Ｚ３、Ｚ４、及びＺ）の１０２４ｂｉｔのデータが発生する。

【００２３】

上述のように、特許文献１に記載された方法では、中間演算データの種類が非常に多くなり、そのｂｉｔ長も５１２ｂｉｔ若しくは１０２４ｂｉｔになる。従って、中間演算データを保持するために、メモリの消費量が多くなってしまう。また、中間演算データをロード又はアンロードするために、時間が費やされてしまう。さらに、図４には、ＲＳＡ暗号の鍵長が１０２４ｂｉｔである場合の例が示されているが、近年利用されるＲＳＡ暗号では、安全性の面から、鍵長が１２８０ｂｉｔ～２０４８ｂｉｔに変わりつつある。従って、更にメモリを多く消費することになる。加えて、特許文献１に記載された方法では、復号処理を行うために乱数を発生させる必要があり、乱数生成器をコンピュータに設ける必要がある。

【００２４】

すなわち、特許文献１に記載された方法では、中間演算処理に要する負担が増大し、中間演算データを一時保存するために大量のメモリが必要になる。また、乱数生成器を設けなければならない。そのため、低価格化が要求されるシステムに対して実装することは不向きである、という問題点があった。

【００２５】

また、既述のように、特別なコプロセッサ（多倍長整数を用いた算術演算を行うコプロセッサ）を用いることにより、メモリの消費量を抑制することは可能であるが、そのようなコプロセッサの回路規模は非常に大きい。従って、コスト増大のインパクトも非常に大きい。低価格化が要求されるシステム（例えば機器認証を必要とするインターネット接続可能な情報家電などに適用されるシステム）に実装する場合は、不利になる。

【課題を解決するための手段】

【００２６】

本発明に係る復号処理装置は、メッセージＭを示すメッセージデータ、秘密素数ｐを示すｐデータ、秘密素数ｑを示すｑデータ、秘密鍵ｄを示すｄデータ、及び、前記ｐ及び前記ｑよりも大きい奇数である秘密変数ｒを示す秘密変数データを格納する、データ記憶部と、事前処理部と、主処理部と、後処理部とを具備する。前記メッセージＭは、平文Ｚ、公開鍵ｅ、及び公開鍵Ｎに基づいて、下記式１２により得られたものである。

（数式１２）：$M = Z^{e} \bmod N$

前記ｅは、（ｐ－１）×（ｑ－１）と互いに素である正の整数である。前記Ｎは、ｐ×ｑにより表される数である。前記ｄは、（ｐ－１）×（ｑ－１）を法とした前記ｅの逆元を示す数である。前記事前処理部は、前記ｐデータ、前記ｑデータ、及び前記ｄデータに基づいて、下記式１３乃至１５によって表される計算を行い、ｕを示すｕデータ、d_pを示すd_pデータ、及びd_qを示すd_qデータを生成する。

（数式１３）：$u = q^{-1} \bmod p$

（数式１４）：$d_p = d \bmod (p-1)$

（数式１５）：$d_q = d \bmod (q-1)$

前記主処理部は、前記メッセージＭ、前記ｐデータ、及び前記ｑデータに基づいて、下記式１６及び１７によって表される計算を行い、M_pを示すM_pデータ、及びM_qを示すM_qデータを生成し、前記M_pデータ、前記d_pデータ、前記ｐデータ、前記M_qデータ、前記d_qデータ、及び前記ｑデータに基づいて、下記式１８及び１９によって表される計算を行い、Ｃｐを示すＣｐデータ及びＣｑを示すＣｑデータを生成する。

（数式１６）：$M_p = M \bmod p$

（数式１７）：$M_q = M \bmod q$

（数式１８）：$Cp = (M_p)^{d_p} \bmod p$

（数式１９）：$Cq = (M_q)^{d_q} \bmod q$

前記後処理部は、前記Ｃｐデータ、前記Ｃｑデータ、前記ｕデータ、及び前記ｐデータに基づいて、下記式２０によって表される計算を行い、Ｃを示すＣデータを生成し、前記Ｃデータ、前記ｑデータ、前記ｒデータ、前記Ｃｑデータに基づいて、下記式２１又は２２によって表される計算を行い、前記平文Ｚを示す出力データを生成する。

（数式２０）：$C = ((C_p - C_q) \times u) \bmod p$

（数式２１）；$Z = (C \times q\,(r+1) + C_q) \bmod qr$

（数式２２）；$Z = (C \times q\,(k \times r + 1) + C_q) \bmod qr$

ここで、上式２２中、ｋは任意の定数を示す。

【００２７】

本発明に係る復号処理方法は、コンピュータが、メッセージＭを示すメッセージデータ、秘密素数ｐを示すｐデータ、秘密素数ｑを示すｑデータ、秘密鍵であるｄを示すｄデータ、及び、前記ｐ及び前記ｑよりも大きい奇数である秘密変数ｒを示す秘密変数データを取得するステップと、コンピュータが、事前処理を行うステップと、コンピュータが、主処理を行うステップと、コンピュータが、後処理を行うステップとを具備する。前記メッセージＭは、平文Ｚ、公開鍵ｅ、及び公開鍵Ｎに基づいて、下記式１２により得られたものである。

（数式１２）：$M = Z^{e} \bmod N$

前記ｅは、（ｐ－１）×（ｑ－１）と互いに素である整数である。前記Ｎは、ｐ×ｑにより表される数である。前記ｄは、（ｐ－１）×（ｑ－１）を法とした前記ｅの逆元を示す数である。前記事前処理を行うステップは、前記ｐデータ、前記ｑデータ、及び前記ｄデータに基づいて、下記式１３乃至１５によって表される計算を行い、ｕを示すｕデータ、d_pを示すd_pデータ、及びd_qを示すd_qデータを生成するステップを含む。

（数式１３）：$u = q^{-1} \bmod p$

（数式１４）：$d_p = d \bmod (p-1)$

（数式１５）：$d_q = d \bmod (q-1)$

前記主処理を行うステップは、前記メッセージＭ、前記ｐデータ、及び前記ｑデータに基づいて、下記式１６及び１７によって表される計算を行い、Ｍｐを示すＭｐデータ、及

びＭｑを示すＭｑデータを生成し、前記M_pデータ、前記d_pデータ、前記ｐデータ、前記M_qデータ、前記d_qデータ、及び前記ｑデータに基づいて、下記式１８及び１９によって表される計算を行い、Ｃｐを示すＣｐデータ及びＣｑを示すＣｑデータを生成ステップを含む。

（数式１６）：$M_p = M \bmod p$

（数式１７）：$M_q = M \bmod q$

（数式１８）：$C_p = (M_p)^{d_p} \bmod p$

（数式１９）：$C_q = (M_q)^{d_q} \bmod q$

前記後処理を行うステップは、前記Ｃｐデータ、前記Ｃｑデータ、前記ｕデータ、及び前記ｐデータに基づいて、下記式２０によって表される計算を行い、Ｃを示すＣデータを生成し、前記Ｃデータ、前記ｑデータ、前記ｒデータ、前記Ｃｑデータに基づいて、下記式２１又は２２によって表される計算を行い、前記平文Ｚを示す出力データを生成するステップを含む。

（数式２０）：$C = ((C_p - C_q) \times u) \bmod p$

（数式２１）；$Z = (C \times q\,(r+1) + C_q) \bmod qr$

（数式２２）；$Z = (C \times q\,(k \times r + 1) + C_q) \bmod qr$

ここで、上式１１中、ｋは任意の定数を示す。

【００２８】

本発明に係る復号処理プログラムは、上述の復号処理方法をコンピュータにより実現するためのプログラムである。

【発明の効果】

【００２９】

本発明によれば、中間演算データのメモリ消費量を削減できる、復号処理装置、復号処理方法、及び復号処理プログラムが提供される。

【図面の簡単な説明】

【００３０】

【図１】ＣＲＴを適用した復号処理を示すフローチャートである。

【図２Ａ】特許文献１に記載された復号処理方法を示すフローチャートである。

【図２Ｂ】ステップＳ１０２における処理を詳細に示すフローチャートである。

【図３】特許文献１に記載された復号処理方法において、記憶装置に格納されるデータを示す構成図である。

【図４】特許文献１において発生する中間演算データを示す概略図である。

【図５】復号処理装置を示す構成図である。

【図６】復号処理プログラムに記載されたアルゴリズムを概略的に示す図である。

【図７】復号処理装置の動作方法を示すフローチャートである。

【図８】発生するデータを概念的に示す図である。

【発明を実施するための形態】

【００３１】

以下に、図面を参照しつつ、本発明の実施形態について説明する。

【００３２】

図５は、本実施形態に係る復号処理装置１を示す構成図である。本実施形態に係る復号処理装置１は、コンピュータによって実現される。図５に示されるように、復号処理装置１は、中央演算処理装置２、データ記憶部３、データ入出力部４、及びプログラム記憶部５を備えている。これらは、データバス６を介して、中央演算処理装置２から復号処理装置１、データ記憶部３、データ入出力部４、プログラム記憶部５にアクセス可能になるように接続されている。

【００３３】

プログラム記憶部５は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）等により実現される。プログラム記憶部５には、復号処理プログラム７が格納されている。復号処理プログラム７は、中央演算処理装置２によって実行される。復号処理プログラム７が実行され

ることにより、事前処理を行う事前処理部８、主処理を行う主処理部９、及び後処理を行なう後処理部１０が実現される。復号処理プログラム７は、例えば、コンピュータによって読み取りが可能な記録媒体（図示せず）から、プログラム記憶部５にインストールされる。

【００３４】

データ入出力部４は、外部装置に接続され、外部装置から必要なデータを取得する機能を有している。また、データ入出力部４は、復号処理装置１によって生成された出力データを外部装置に出力する機能も有している。

【００３５】

データ記憶部３は、復号処理に必要なデータを格納する部分である。データ記憶部３には、入出力データ、及び中間演算データが記憶される。入出力データは、データ入出力部４を介して入出力されるデータである。中間演算データは、復号処理プログラム７の実行中に発生するデータであり、データ記憶部３に一時的に記憶される。

【００３６】

続いて、本実施形態に係る復号処理装置１の動作方法について説明する。まず、本実施形態に係る復号処理装置１の動作方法の概要について説明する。

【００３７】

図６は、復号処理プログラム７に記載されたアルゴリズムを概略的に示す図である。本実施形態では、中央演算処理装置２が復号処理プログラム７を実行することにより、メッセージＭが復号され、平文Ｚが得られる。ここで、メッセージＭは、公開鍵ｅ及びＮを用いて平文Ｚを暗号化することにより、得られたものである。復号処理装置１は、図６に示されるように、秘密鍵ｄ、ｐ、ｑ、ｒ、およびメッセージＭ（暗号文）をパラメータとして用い、平文Ｚを得る。ここで、秘密鍵ｐ及びｑは、素数である。また、秘密鍵ｒは、ｐ及びｑよりも大きい奇数である。また、公開鍵ｅは、（ｐ－１）×（ｑ－１）と互いに素である正の整数である。また、公開鍵Ｎは、ｐ×ｑにより表される数である。更に、秘密鍵ｄは、（ｐ－１）×（ｑ－１）を法としたｅの逆元を示す数である。

【００３８】

図６に示されるように、復号処理装置１では、事前処理部８が事前処理を行い、ｕ、ｄｐ、及びｄｑが求められる。更に、主処理部９によって、Ｍｐ、Ｍｑ、Ｃｐ、及びＣｑが求められる。更に、後処理部１０によって、Ｃ及びＺが求められる。ここで、本実施形態においては、Ｚを計算する為の処理が、工夫されている。すなわち、ＣＲＴを用いた場合の最後の計算式（既述の数式１１）が、下記式２３により計算される。

（数式２３）：Ｚ＝（Ｃ×ｑ（ｒ＋１）＋Ｃｑ）ｍｏｄｑｒ

【００３９】

上式２３を用いることにより、中間演算データの発生量を抑制した上で、電力差分解析攻撃に対する耐性を強化できる。

【００４０】

以下に、復号処理装置１の動作方法について、詳細に説明する。図７は、復号処理装置１の動作方法を示すフローチャートである。

【００４１】

＜ステップＳ１＞

まず、データ入出力部４が、外部から、秘密鍵ｐを示すｐデータ、秘密鍵ｑを示すｑデータ、及び秘密鍵ｄを示すｄデータを取得する。ｐデータ、ｑデータ、及びｄデータは、入出力データとして、データ記憶部３に格納される。

【００４２】

＜ステップＳ２＞

次いで、事前処理部８が、事前処理を実行する。具体的には、事前処理部８は、ｑデータ及びｐデータを用いて、ｐを法としたｑの逆元ｕを計算し、数値ｕを示すｕデータを生成する。また、事前処理部８は、ｐデータ及びｄデータに基づいて、ｐ－１を法としたｄの剰余ｄｐを計算し、数値ｄｐを示すｄｐデータを生成する。更に、事前処理部８は、ｑ

データ及びｄデータに基づいて、ｑ－１を法としたｄの剰余ｄｑを計算し、数値ｄｑを示すｄｑデータを生成する。ｕデータ、ｄｐデータ、及びｄｑデータは、中間演算データとして、データ記憶部３に格納される。

【００４３】

＜ステップＳ３＞

次いで、データ入出力部４が、外部から、メッセージＭを示すＭデータを取得する。Ｍデータは、入出力データとして、データ記憶部３に格納される。

【００４４】

＜ステップＳ４、５＞

次いで、主処理部９が、Ｍデータ及びｐデータに基づいて、Ｍのｐを法とした剰余Ｍｐを計算し、数値Ｍｐを示すＭｐデータを生成する。また、主処理部９は、Ｍデータ及びｑデータに基づいて、Ｍのｑを法とした剰余Ｍｑを計算し、数値Ｍｑを示すＭｑデータを生成する。Ｍｐデータ及びＭｑデータは、中間演算データとして、データ記憶部３に格納される（ステップＳ４）。

【００４５】

また、主処理部９は、Ｍｐデータ、ｄｐデータ、およびｐデータに基づいて、ｄｐを指数かつｐを法としたＭｐのべき乗剰余Ｃｐを計算し、数値Ｃｐを示すＣｐデータを生成する。また、主処理部９は、Ｍｑデータ、ｄｑデータ、及びｑデータに基づいて、ｄｐを指数かつｑを法としたＭｑのべき乗剰余Ｃｑを計算し、数値Ｃｑを示すＣｑデータを生成する。Ｃｐデータ及びＣｑデータは、中間演算データとして、データ記憶部３に格納される（ステップＳ５）。

【００４６】

＜ステップＳ６＞

続いて、後処理部１０が、Ｃｐデータ、Ｃｑデータ、ｕデータ、及びｐデータに基づいて、C_pからC_qを減じた結果にｕを乗じ、その結果のｐを法とした剰余Ｃを計算し、数値Ｃを示すＣデータを生成する。Ｃデータは、中間演算データとして、データ記憶部３に格納される。

【００４７】

＜ステップＳ７＞

続いて、データ入出力部４が、外部装置から、秘密変数ｒを示すｒデータを受信し、データ記憶部３に格納する。秘密変数ｒは、秘密鍵ｐ、ｑよりも大きい奇数である（ステップＳ７）。

【００４８】

＜ステップＳ８～１１＞

続いて、ステップＳ７乃至１１の処理が行われ、既述の式２３「Ｚ＝（Ｃ×ｑ（ｒ＋１）＋Ｃｑ）ｍｏｄｑｒ」の計算が実行される。

【００４９】

すなわち、まず、後処理部１０が、ｑデータ及びｒデータに基づいて、ｑとｒ＋１の乗算m_0を計算し、数値m_0を示すm_0データを生成する。m_0データは、中間演算データとして、データ記憶部３に格納される（ステップＳ８）。

【００５０】

次いで、後処理部１０が、Ｃデータ及びm_0データに基づいて、Ｃとm_0の乗算m_1を計算し、数値m_1を示すm_1データを生成する。m_1データは、中間演算データとして、データ記憶部３に格納される（ステップＳ９）。

【００５１】

次いで、後処理部１０が、m_1データ及びＣｑデータに基づいて、m_1とC_qの加算m_2を計算し、数値m_2を示すm_2データを生成する。m_2データは、中間演算データとして、データ記憶部３に格納される（ステップＳ１０）。

【００５２】

次いで、後処理部１０が、m_2データ、ｑデータ、及びｒデータに基づいて、m_2のｑ

ｒを法とした剰余Ｚを計算し、数値Ｚを示すＺデータを生成する。Ｚデータは、入出力データとして、データ記憶部３に格納される（ステップＳ１１）。

【００５３】

＜ステップＳ１２＞

以上のステップＳ１１までの処理により、平文Ｚを示すＺデータが生成される。Ｚデータは、復号結果として、データ入出力部４を介して外部装置に送信される。

【００５４】

続いて、本実施形態の作用効果について説明する。

【００５５】

既述のように、ＣＲＴを用いた場合の復号処理においては、最後の演算である数式１１「Ｚ＝Ｃ×ｑ＋Ｃｑ」が、電力差分解析攻撃に対して耐性が低い。ここで、本実施形態においては、数式１１が、既述の数式２３「Ｚ＝（Ｃ×ｑ（ｒ＋１）＋Ｃｑ）ｍｏｄｑｒ」に変形されている。秘密変数ｒが用いられているため、電力差分解析攻撃によって秘密鍵ｑを予測するためには、攻撃者は、秘密変数ｒも予測する必要がある。２つの秘密変数ｑ及びｒを予測する必要があるので、電力差分解析攻撃によって秘密鍵ｑを推測することが困難になる。従って、電力差分解析攻撃に対する耐性を高めることができる。

【００５６】

尚、式１１と式２３とが等価であることは、以下の式展開により、理解できる。

Ｚ＝（Ｃ×ｑ（ｒ＋１）＋Ｃｑ）ｍｏｄｑｒ

＝（Ｃ×ｑｒ＋Ｃ×ｑ＋Ｃｑ）ｍｏｄｑｒ

＝０＋（Ｃ×ｑ＋Ｃｑ）ｍｏｄｑｒ

＝Ｃ×ｑ＋Ｃｑ

∵Ｃ＜ｐ、Ｃｑ＜ｑ、Ｐ＜ｒより、（Ｃ×ｑ＋Ｃｑ）＜ｑｒは明確。

【００５７】

また、式２３の代わりに、任意の整数ｋを用いて、下記式２４を用いても、同様の結果を得ることができる。

（数式２４）：Ｚ＝（Ｃ×ｑ（ｋ×ｒ＋１）＋Ｃｑ）ｍｏｄｑｒ

【００５８】

加えて、本実施形態によれば、復号処理時に発生する中間演算データのデータ量を抑制することができる。以下に、この点について詳述する。

【００５９】

図８は、本実施形態において発生するデータを概念的に示す図である。図８に示されるように、本実施形態では、入力データとして、ｐデータ、ｑデータ、ｄデータ、ｒデータ、及びＭデータが用いられる。ここで、ｐデータ、ｑデータ、ｄデータ、及びｒデータは、それぞれ５１２ｂｉｔであるものとする。また、Ｍデータは、１０２４ｂｉｔであるものとする。すなわち、鍵長は、１０２４ｂｉｔであるものとする。

【００６０】

図８に示されるように、中間演算データとしては、ｕデータ，d_pデータ，d_qデータ，M_pデータ，M_qデータ，C_pデータ，C_qデータ，C_0データ，Ｃデータ，r_1データ、C_1データ、m_0データ、m_1データ、m_2データ、及びＫデータが発生する。ここで、ｕデータ，d_pデータ，d_qデータ，M_pデータ，M_qデータ，C_pデータ，C_qデータ，C_0データ，Ｃデータ及びr_1データは、それぞれ、５１２ｂｉｔである。また、C_1データ，m_0データ，及びＫデータは、１０２４ｂｉｔである。また、m_1データ、およびm_2データは、それぞれ、１５３６ｂｉｔである。尚、Ｚデータは、１０２４ｂｉｔである。すなわち、１０個の５１２ｂｉｔのデータ、４個の１０２４ｂｉｔのデータ、及び２個の１５３６ｂｉｔのデータが発生する。すなわち、本実施形態においては、メモリ消費量は、１２Ｋｂｉｔである。

【００６１】

本実施形態を図３に示した例と比較する。図３に示した例では、メモリ消費量は、１５Ｋｂｉｔである。すなわち、本実施形態によれば、図３に示した例と比較して、メモリ消

費量を、３Ｋｂｉｔほど削減できることが理解される。すなわち、本実施形態では、既述の式１０及び式１１のうち、式１１だけが変形されているため、式１０及び式１１の双方を変形する場合と比較して、メモリ消費量を小さくすることができる。

【００６２】

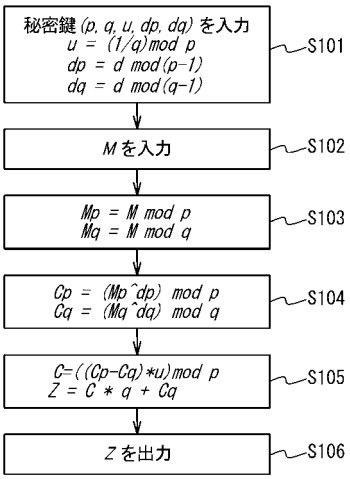
以上説明したように、本実施形態によれば、メモリ消費量を抑制した上で、電力差分解析攻撃に対する耐性を向上することができる。メモリ消費量が削減できるため、中間演算データをロード及びアンロードするために費やされる時間も削減できる。また、乱数生成器を設ける必要がないため、低価格化を実現できる。従って、低価格化が要求されるシステムに対して、有効に適用することができる。

【符号の説明】

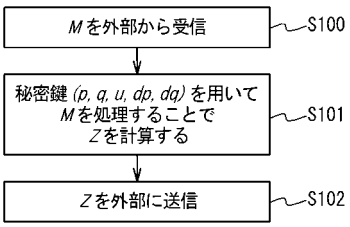
【００６３】

１　復号処理装置
２　中央演算処理装置
３　データ記憶部
４　データ入出力部
５　プログラム記憶部
６　データバス
７　復号プログラム
８　事前処理部
９　主処理部
１０　後処理部

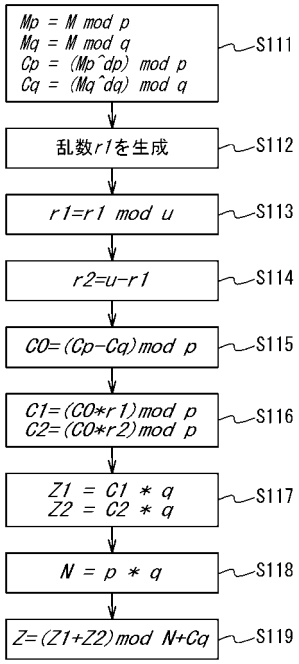
【図１】



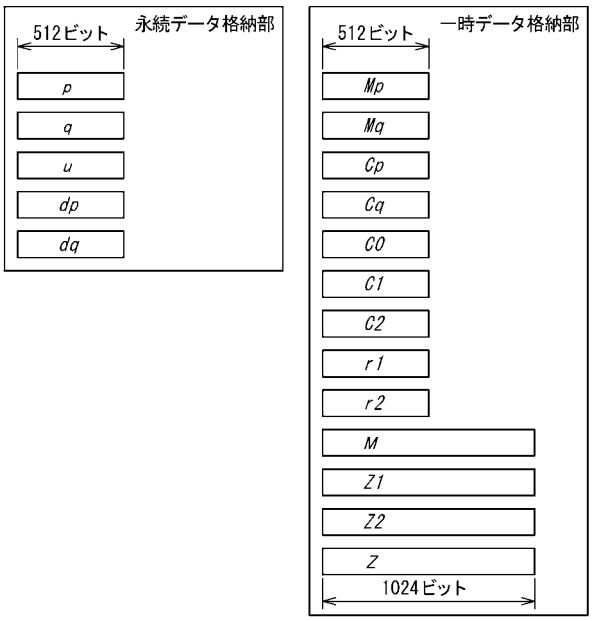
【図２Ａ】



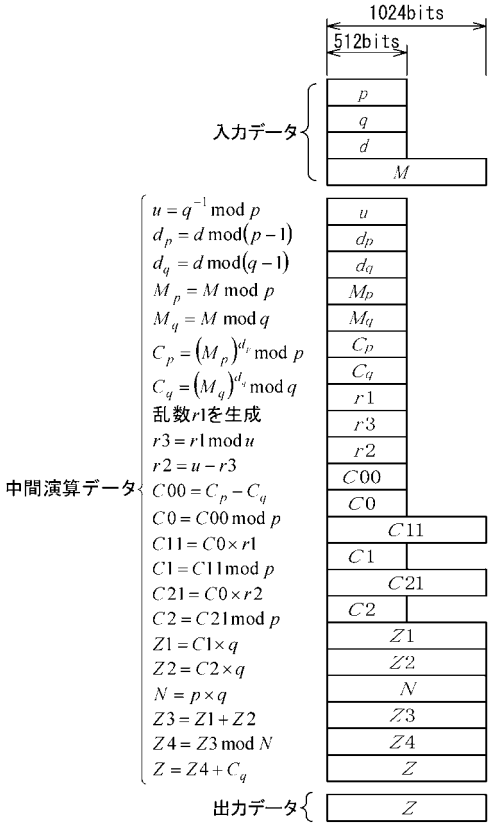
【図２Ｂ】



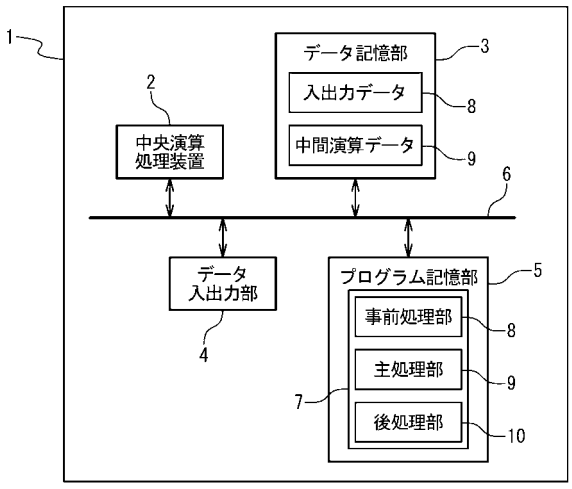
【図３】



【図４】



【図５】



【図６】

パラメータ

秘密鍵：d, p, q, r　（p, qは素数、rは奇数、$p, q < r$）
暗号文：M

事前処理

$u = q^{-1} \bmod p$
$d_p = d \bmod (p-1)$
$d_q = d \bmod (q-1)$

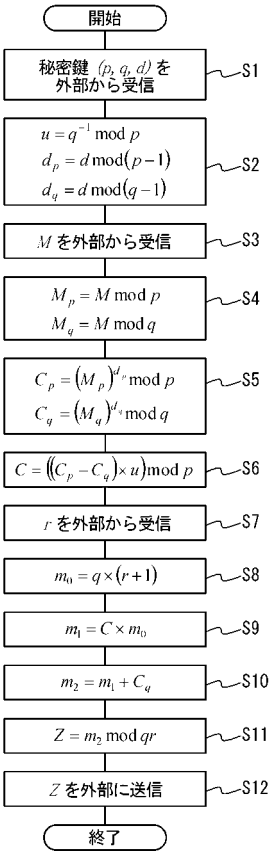
主処理

$M_p = M \bmod p$
$M_q = M \bmod q$
$C_p = (M_p)^{d_p} \bmod p$
$C_q = (M_q)^{d_q} \bmod q$

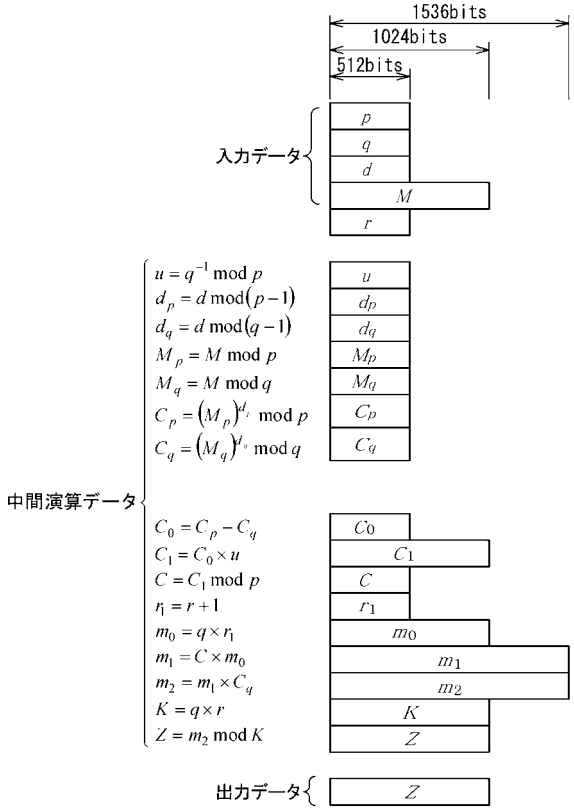
後処理

$C = ((C_p - C_q) \times u) \bmod p$
$Z = (C \times q(r+1) + C_q) \bmod qr$

【図７】


開始
秘密鍵 (p, q, d) を外部から受信
S1
$u = q^{-1} \bmod p$
$d_p = d \bmod (p-1)$
$d_q = d \bmod (q-1)$
S2
M を外部から受信
S3
$M_p = M \bmod p$
$M_q = M \bmod q$
S4
$C_p = (M_p)^{d_p} \bmod p$
$C_q = (M_q)^{d_q} \bmod q$
S5
$C = ((C_p - C_q) \times u) \bmod p$
S6
r を外部から受信
S7
$m_0 = q \times (r+1)$
S8
$m_1 = C \times m_0$
S9
$m_2 = m_1 + C_q$
S10
$Z = m_2 \bmod qr$
S11
Z を外部に送信
S12
終了

【図８】


1536bits
1024bits
512bits
入力データ
p
q
d
M
r
中間演算データ
$u = q^{-1} \bmod p$
$d_p = d \bmod (p-1)$
$d_q = d \bmod (q-1)$
$M_p = M \bmod p$
$M_q = M \bmod q$
$C_p = (M_p)^{d_p} \bmod p$
$C_q = (M_q)^{d_q} \bmod q$
u
d_p
d_q
M_p
M_q
C_p
C_q
$C_0 = C_p - C_q$
$C_1 = C_0 \times u$
$C = C_1 \bmod p$
$r_1 = r + 1$
$m_0 = q \times r_1$
$m_1 = C \times m_0$
$m_2 = m_1 \times C_q$
$K = q \times r$
$Z = m_2 \bmod K$
C_0
C_1
C
r_1
m_0
m_1
m_2
K
Z
出力データ
Z