

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02008/013154

発行日 平成21年12月17日 (2009.12.17)

(43) 国際公開日 平成20年1月31日 (2008.1.31)

(51) Int.Cl.	F I	テーマコード (参考)
<b>G09C 1/00 (2006.01)</b>	G09C 1/00 650A	5J104
	G09C 1/00 660D	

審査請求 未請求 予備審査請求 未請求 (全 27 頁)

出願番号 特願2008-526767 (P2008-526767)	(71) 出願人 504147243 国立大学法人 岡山大学 岡山県岡山市北区津島中一丁目1番1号
(21) 国際出願番号 PCT/JP2007/064474	
(22) 国際出願日 平成19年7月24日 (2007.7.24)	
(31) 優先権主張番号 特願2006-200946 (P2006-200946)	(74) 代理人 100080160 弁理士 松尾 憲一郎
(32) 優先日 平成18年7月24日 (2006.7.24)	
(33) 優先権主張国 日本国 (JP)	(72) 発明者 野上 保之 岡山県岡山市津島中三丁目1番1号 岡山 大学大学院自然科学研究科内
(31) 優先権主張番号 特願2007-10072 (P2007-10072)	(72) 発明者 森川 良孝 岡山県岡山市津島中三丁目1番1号 岡山 大学大学院自然科学研究科内
(32) 優先日 平成19年1月19日 (2007.1.19)	
(33) 優先権主張国 日本国 (JP)	

Fターム(参考) 5J104 AA21 JA21 JA23 NA02 NA17 NA39

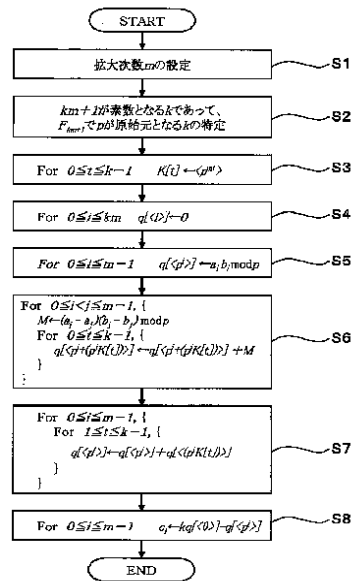
最終頁に続く

(54) 【発明の名称】 暗号化/復号化プログラム、暗号化/復号化装置及び拡大体の乗算装置

(57) 【要約】

任意な鍵長を選択可能としながら高速に拡大体の乗算処理を実行可能とした暗号化/復号化プログラム、暗号化/復号化装置、及び拡大体の乗算装置を提供する。

素数  $p$  を標数とし、拡大次数  $m$  の拡大体  $F_p^m$  の 2 つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$  を乗算する際に、 $km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を特定し、2 つの元  $A$ 、 $B$  を、正整数  $k$  を用いて素数  $p$  を標数とする拡大次数  $km$  の拡大体  $F_p^{km}$  における 2 つの元として演算し、この演算結果を用いて部分体である拡大次数  $m$  の拡大体  $F_p^m$  の元における乗算の結果を求める。



S1 SET EXTENSION DEGREE  $m$   
 S2 SPECIFY  $k$  SUCH THAT  $km+1$  IS PRIME NUMBER  
 AND  $p$  IS PRIMITIVE NUMBER IN  $F_{km+1}$

## 【特許請求の範囲】

## 【請求項 1】

素数  $p$  を標数とし、拡大次数  $m$  の拡大体  $F_p^m$  の 2 つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$  を、平文データと暗号化鍵、または暗号データと復号化鍵として、

電子計算機で、前記平文データと前記暗号化鍵とを乗算して暗号データの元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成させる、または前記暗号データと前記復号化鍵とを乗算して平文データの元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成させる暗号化 / 復号化プログラムにおいて、

$km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を特定する第 1 のステップと

10

前記の 2 つの元  $A$ 、 $B$  を、前記正整数  $k$  を用いて素数  $p$  を標数とする拡大次数  $km$  の拡大体  $F_p^{km}$  における 2 つの元として乗算を行う第 2 のステップと、

この乗算の結果を用いて部分体である前記拡大次数  $m$  の拡大体  $F_p^m$  の元における乗算の結果を求める第 3 のステップと

を有することを特徴とする暗号化 / 復号化プログラム。

## 【請求項 2】

$0 \leq i < m-1$ 、 $0 \leq j < k-1$  とし、

$\langle x \rangle$  が  $x$  の  $\text{mod}(km+1)$  をとるものとして、

前記第 2 のステップは、

$0 \leq t < k-1$  で、 $\langle p^{mi} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めるステップと、

$0 \leq i < km$  で、それぞれ  $0 = q[\langle i \rangle]$  とするステップと、

$0 \leq i < m-1$  で、 $a_i b_i \text{ mod } p = q[\langle p^i \rangle]$  をそれぞれ求めるステップと、

$0 \leq i < j < m-1$  で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$  をそれぞれ求めて、 $0 \leq t < k-1$  で  $q[\langle p^i + (p^j K[t]) \rangle]$  に  $M$  をそれぞれ足し込むステップと

を有することを特徴とする請求項 1 記載の暗号化 / 復号化プログラム。

20

## 【請求項 3】

前記第 3 のステップは、

$0 \leq i < m-1$  で、かつ  $1 \leq t < k-1$  で、 $q[\langle p^i \rangle]$  に  $q[\langle (p^i K[t]) \rangle]$  をそれぞれ足し込むステップと、

30

$0 \leq i < m-1$  で、 $kq[\langle 0 \rangle] - q[\langle p^i \rangle] = c_i$  をそれぞれ求めるステップと

を有することを特徴とする請求項 2 記載の暗号化 / 復号化プログラム。

## 【請求項 4】

$k=2k'$  の場合に、

$F_{2k'm+1}$  で  $p$  が原始元あるいは位数が  $k'm$  かつ  $k'm$  が奇数となる正整数  $k'$  とし、

$0 \leq i < m-1$ 、 $0 \leq j < 2k'-1$  とし、

$\langle x \rangle$  が  $x$  の  $\text{mod}(2k'm+1)$  をとるものとして、

前記第 2 のステップは、

$0 \leq t < k'-1$  で、 $\langle p^{mi} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めるステップと、

$0 \leq i < 2k'm$  で、それぞれ  $0 = q[\langle i \rangle]$  とするステップと、

40

$0 \leq i < m-1$  で、 $a_i b_i \text{ mod } p = q[\langle p^i \rangle]$  をそれぞれ求めるステップと、

$0 \leq i < j < m-1$  で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$  をそれぞれ求めて、 $0 \leq t < k'-1$  で  $q[\langle p^i + (p^j K[t]) \rangle]$  に  $M$  をそれぞれ足し込むとともに、 $q[\langle p^i - (p^j K[t]) \rangle]$  に  $M$  をそれぞれ足し込むステップと

を有することを特徴とする請求項 1 記載の暗号化 / 復号化プログラム。

## 【請求項 5】

前記第 3 のステップは、

$0 \leq i < m-1$  で、かつ  $1 \leq t < k'-1$  で、 $q[\langle p^i \rangle]$  に  $q[\langle (p^i K[t]) \rangle]$  をそれぞれ足し込むとともに、 $q[\langle p^i \rangle]$  に  $q[\langle -(p^i K[t]) \rangle]$  をそれぞれ足し込むステップと、

$0 \leq i < m-1$  で、 $-q[\langle p^i \rangle] = c_i$  をそれぞれ求めるステップと

50

を有することを特徴とする請求項 4 記載の暗号化 / 復号化プログラム。

【請求項 6】

素数  $p$  を標数とし、拡大次数  $m$  の拡大体  $F_p^m$  の 2 つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$  を、平文データと暗号化鍵、または暗号データと復号化鍵として、

前記平文データと前記暗号化鍵とを乗算させて元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成することにより暗号化する、または前記暗号データと前記復号化鍵とを乗算させて元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成することにより復号化する演算器を備えた暗号化 / 復号化装置において、

前記元をそれぞれ記憶する第 1 の記憶部と、

前記拡大次数  $m$  を記憶する第 2 の記憶部と、

$km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を前記演算器による演算に基づいて特定して記憶する第 3 の記憶部と、

前記の 2 つの元  $A$ 、 $B$  を、前記正整数  $k$  を用いて素数  $p$  を標数とする拡大次数  $km$  の拡大体  $F_p^{km}$  における 2 つの元として前記演算器で乗算した結果を記憶する第 4 の記憶部と、

前記拡大次数  $km$  の拡大体  $F_p^{km}$  の元の乗算結果を用いて前記演算器で所定の演算を行って、部分体である前記拡大次数  $m$  の拡大体  $F_p^m$  の元における乗算の結果を求めて記憶する第 5 の記憶部と

を有することを特徴とする暗号化 / 復号化装置。

【請求項 7】

$0 \leq i \leq m-1$ 、 $0 \leq j \leq k-1$  とし、

$\langle x \rangle$  が  $x$  の  $\text{mod}(km+1)$  をとるものとして、

前記第 4 の記憶部は、

$0 \leq t \leq k-1$  で、 $\langle p^{mt} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めて記憶する記憶部と、

$0 \leq i \leq km$  で、それぞれ  $0 \leq q \leq \langle i \rangle$  として記憶する記憶部と、

$0 \leq i \leq m-1$  で、 $a_i b_i \text{ mod } p = q \langle p^i \rangle$  をそれぞれ求めて記憶する記憶部と、

$0 \leq i < j \leq m-1$  で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$  をそれぞれ求めて記憶する記憶部と、

$0 \leq t \leq k-1$  で  $q \langle p^i + (p^i K[t]) \rangle$  に  $M$  をそれぞれ足し込んで記憶する記憶部と

を有することを特徴とする請求項 6 記載の暗号化 / 復号化装置。

【請求項 8】

前記第 5 の記憶部は、

$0 \leq i \leq m-1$  で、かつ  $1 \leq t \leq k-1$  で、 $q \langle p^i \rangle$  に  $q \langle (p^i K[t]) \rangle$  をそれぞれ足し込んで記憶する記憶部と、

$0 \leq i \leq m-1$  で、 $kq \langle 0 \rangle - q \langle p^i \rangle = c_i$  をそれぞれ求めて記憶する記憶部と

を有することを特徴とする請求項 7 記載の暗号化 / 復号化装置。

【請求項 9】

$k=2k'$  の場合に、

$F_{2k'm+1}$  で  $p$  が原始元あるいは位数が  $k'm$  かつ  $k'm$  が奇数となる正整数  $k'$  として、この正整数  $k'$  を記憶する記憶部を有し、

$0 \leq i \leq m-1$ 、 $0 \leq j \leq 2k'-1$  とし、

$\langle x \rangle$  が  $x$  の  $\text{mod}(2k'm+1)$  をとるものとして、

前記第 4 の記憶部は、

$0 \leq t \leq k'-1$  で、 $\langle p^{mt} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めて記憶する記憶部と、

$0 \leq i \leq 2k'm$  で、それぞれ  $0 \leq q \leq \langle i \rangle$  として記憶する記憶部と、

$0 \leq i \leq m-1$  で、 $a_i b_i \text{ mod } p = q \langle p^i \rangle$  をそれぞれ求めて記憶する記憶部と、

$0 \leq i < j \leq m-1$  で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$  をそれぞれ求めて記憶する記憶部と、

$0 \leq t \leq k'-1$  で  $q \langle p^i + (p^i K[t]) \rangle$  に  $M$  をそれぞれ足し込んで記憶するとともに、 $q \langle p^i - (p^i K[t]) \rangle$  に  $M$  をそれぞれ足し込んで記憶する記憶部と

を有することを特徴とする請求項 6 記載の暗号化 / 復号化装置。

【請求項 10】

10

20

30

40

50

前記第 5 の記憶部は、

$0 \leq i \leq m-1$ で、かつ  $1 \leq t \leq k-1$ で、 $q[\langle p^i \rangle]$ に $q[\langle (p^i K[t]) \rangle]$ をそれぞれ足し込むとともに、 $q[\langle p^i \rangle]$ に $q[\langle -(p^i K[t]) \rangle]$ をそれぞれ足し込んで記憶する記憶部と、

$0 \leq i \leq m-1$ で、 $-q[\langle p^i \rangle] = c_i$ をそれぞれ求めて記憶する記憶部と

を有することを特徴とする請求項 9 記載の暗号化 / 復号化装置。

【請求項 11】

素数  $p$  を標数とし、拡大次数  $m$  の拡大体  $F_p^m$  の 2 つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$  を乗算して元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成する演算器を備えた拡大体の乗算装置において、

前記元をそれぞれ記憶する第 1 の記憶部と、

前記拡大次数  $m$  を記憶する第 2 の記憶部と、

$km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を前記演算器による演算に基づいて特定して記憶する第 3 の記憶部と、

前記の 2 つの元  $A$ 、 $B$  を、前記正整数  $k$  を用いて素数  $p$  を標数とする拡大次数  $km$  の拡大体  $F_p^{km}$  における 2 つの元として前記演算器で乗算した結果を記憶する第 4 の記憶部と、

前記拡大次数  $km$  の拡大体  $F_p^{km}$  の元の乗算結果を用いて前記演算器で所定の演算を行って、部分体である前記拡大次数  $m$  の拡大体  $F_p^m$  の元における乗算の結果を求めて記憶する第 5 の記憶部と

を有することを特徴とする拡大体の乗算装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、暗号化 / 復号化プログラム、暗号化 / 復号化装置、及び暗号化または復号化における乗算処理を実行する拡大体の乗算装置に関する。

【背景技術】

【0002】

従来、インターネットなどの電気通信回線を利用した情報通信において、送受信されるデータの秘匿性を保持するために、データの暗号化が行われている。すなわち、平文データを送信する送信者は、平文データに暗号化処理を施して暗号データを生成し、この暗号データを受信者に送信している。一方、暗号データを受信した受信者は、暗号データに復号化処理を施して平文データを生成することにより、平文データを受け取ることができる。

【0003】

このような暗号化及び復号化の方法として、昨今では公開鍵暗号と呼ばれる方法が用いられている。公開鍵暗号では、公開鍵と秘密鍵があらかじめ設定され、所定の平文データを送信する送信者に公開鍵を開示しており、送信者は公開鍵を用いて平文データを暗号化することにより暗号データを生成し、受信者に送信している。受信者は、暗号データを受信すると、秘密鍵を用いて暗号データを復号化して平文データを生成している。

【0004】

ここで、平文データを暗号化する場合には、平文データを暗号化に用いる公開鍵の鍵長に合わせた所定のデータ長ごとに分断して複数の単位長平文データを生成し、各単位長平文データと公開鍵を用いて乗算処理を行うことにより単位長暗号データを生成し、所定数の単位長暗号データで構成された暗号データを生成している。

【0005】

一方、暗号データを復号化する場合には、暗号データを復号化に用いる秘密鍵の鍵長に合わせた所定のデータ長ごとに分断して複数の単位長暗号データを生成し、各単位長暗号データと秘密鍵を用いて乗算処理を行うことにより単位長平文データを生成し、所定数の単位長平文データで構成された平文データを生成している。

【0006】

このような公開鍵暗号には様々な方式が提案されており、Rivest Shamir Adleman (R

10

20

30

40

50

S A ) 暗号、楕円曲線暗号、ElGamal 暗号などが知られている。

【 0 0 0 7 】

昨今、パーソナルコンピュータなどの電子計算機の性能向上にともなって、各種の暗号方法で暗号化された暗号データが解読されるおそれが高まっている。すなわち、暗号データは、秘密鍵さえ分かれば解読できることから、電子計算機によって手当たり次第に秘密鍵を生成して復号化を試みることにより、時間はかかるものの解読されるおそれがあった。

【 0 0 0 8 】

そこで、各暗号方法では、安全性を高めるために公開鍵及び秘密鍵の鍵長を長くすることが行われている。すなわち、公開鍵及び秘密鍵の鍵長を長くすると、解読に用いる秘密鍵の数が飛躍的に増大し、現実的な時間内での解読を不可能とすることができるからである。そのため、現在では、R S A 暗号では 1 0 2 4 ビット以上、楕円曲線暗号では 1 6 0 ビット以上、ElGamal 暗号では 1 0 2 4 ビット以上の鍵長が求められている。

10

【 0 0 0 9 】

しかしながら、公開鍵及び秘密鍵の鍵長を長くした場合には、公開鍵を用いた乗算処理による暗号化、及び秘密鍵を用いた乗算処理による復号化に多大な時間を要することとなっていた。この場合、処理時間の短縮のためには、乗算処理の演算速度が高速な演算手段が必要となることにより、安全性を高めるためのコストが増大することとなっていた。

【 0 0 1 0 】

一方で、現実的には、電気通信回線中を流れているデータにおいては重要度が様々に異なっており、利用価値が高いために高度の秘匿性が必要なデータから、利用価値が低いために秘匿性を必要としないデータまでが存在している。

20

【 0 0 1 1 】

したがって、何れのデータに対しても同等の安全性で暗号化する必要はなく、高い安全性が要求されるデータには長い鍵長の公開鍵及び秘密鍵を用い、高い安全性が要求されないデータには短い鍵長の公開鍵及び秘密鍵が用いられている。

【 0 0 1 2 】

また、パーソナルコンピュータなどのような高速な演算処理の実行が可能な装置では、できるだけ長い鍵長の公開鍵及び秘密鍵による暗号化が利用されており、携帯電話機や IC カードなどのような演算処理能力の乏しい装置では、比較的短い鍵長の公開鍵及び秘密鍵による暗号化が利用され、保証され得る安全性の範囲内でデータの送受信が行われている。

30

【 0 0 1 3 】

特に、パーソナルコンピュータなどの電子計算機では、複数種類の鍵長の公開鍵及び秘密鍵が利用可能となっており、送信するデータに応じた安全性、あるいは送信先の装置における乗算処理の処理能力などに応じて鍵長を変えて暗号化することも行われており、鍵長に汎用性を持たせることが提案されている（例えば、特許文献 1 参照。 ）。

【特許文献 1】特開 2 0 0 1 - 0 5 1 8 3 2 号公報

【発明の開示】

【発明が解決しようとする課題】

40

【 0 0 1 4 】

しかしながら、通常、鍵長の決定にともなって、乗算処理などの演算処理に必要な拡大体が、所定の拡大体に特定されてしまうために、鍵長に汎用性を持たせた場合には、鍵長ごとの拡大体をあらかじめ準備しておかなければならなかった。したがって、鍵長の汎用性を高めようとするればするほど、鍵長に対応した拡大体を記憶しておくためのより大きな記憶領域が必要となっていた。

【 0 0 1 5 】

したがって、現実的には、準備できる記憶領域の大きさの制限から、鍵長は 3 ~ 5 種類程度しか準備されておらず、必ずしも十分な汎用性が提供できてはいなかった。そのため、準備された鍵長の公開鍵及び秘密鍵では安全性が十分に保証できない状態となった場合

50

に、安全性をさらに高めることはできなかった。

【0016】

しかも、従来の暗号化または復号化における乗算処理では、多項式積の計算の後に多項式剰余算の計算が必要であって、多項式積の計算が終了するまでは多項式剰余算の計算を開始することができなかった。したがって、このような乗算処理を演算回路を構成して実行する場合には、演算回路の並列化が困難であって、処理速度の高速化を図りにくいという問題もあった。

【0017】

本発明者らは、このような現状に鑑み、任意な鍵長を選択可能としながら高速に乗算処理を実行可能とすることにより、利便性の高い暗号化及び復号化のシステムを構築可能とするために研究を行って、本発明を成すに至ったものである。

10

【課題を解決するための手段】

【0018】

本発明の暗号化／復号化プログラムでは、素数  $p$  を標数とし、拡大次数  $m$  の拡大体  $F_p^m$  の2つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$  を、平文データと暗号化鍵、または暗号データと復号化鍵として、電子計算機で、平文データと暗号化鍵とを乗算して暗号データの元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成させる、または暗号データと復号化鍵とを乗算して平文データの元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成させる暗号化／復号化プログラムにおいて、 $km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を特定する第1のステップと、2つの元  $A$ 、 $B$  を、正整数  $k$  を用いて素数  $p$  を標数とする拡大次数  $km$  の拡大体  $F_p^{km}$  における2つの元として乗算を行う第2のステップと、この乗算の結果を用いて部分体である拡大次数  $m$  の拡大体  $F_p^m$  の元における乗算の結果を求める第3のステップとを有することとした。

20

【0019】

さらに、本発明の暗号化／復号化プログラムでは、

$0 \leq i \leq m-1$ 、 $0 \leq j \leq k-1$  とし、

$\langle x \rangle$  が  $x$  の  $\text{mod}(km+1)$  をとるものとして、

第2のステップが、

$0 \leq t \leq k-1$  で、 $\langle p^{mt} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めるステップと、

$0 \leq i \leq km$  で、それぞれ  $0 = q[\langle i \rangle]$  とするステップと、

$0 \leq i \leq m-1$  で、 $a_i b_i \text{ mod } p = q[\langle p^i \rangle]$  をそれぞれ求めるステップと、

$0 \leq i < j \leq m-1$  で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$  をそれぞれ求めて、 $0 \leq t \leq k-1$  で  $q[\langle p^i + (p^j K[t]) \rangle]$  に  $M$  をそれぞれ足し込むステップと

を有することにも特徴を有するものであり、

第3のステップが、

$0 \leq i \leq m-1$  で、かつ  $1 \leq t \leq k-1$  で、 $q[\langle p^i \rangle]$  に  $q[\langle (p^i K[t]) \rangle]$  をそれぞれ足し込むステップと、

$0 \leq i \leq m-1$  で、 $kq[\langle 0 \rangle] - q[\langle p^i \rangle] = c_i$  をそれぞれ求めるステップと

を有することにも特徴を有するものである。

30

【0020】

さらに、本発明の暗号化／復号化プログラムでは、

$k=2k'$  の場合に、

$F_{2k'm+1}$  で  $p$  が原始元あるいは位数が  $k'm$  かつ  $k'm$  が奇数となる正整数  $k'$  とし、

$0 \leq i \leq m-1$ 、 $0 \leq j \leq 2k'-1$  とし、

$\langle x \rangle$  が  $x$  の  $\text{mod}(2k'm+1)$  をとるものとして、

第2のステップが、

$0 \leq t \leq k'-1$  で、 $\langle p^{mt} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めるステップと、

$0 \leq i \leq 2k'm$  で、それぞれ  $0 = q[\langle i \rangle]$  とするステップと、

$0 \leq i \leq m-1$  で、 $a_i b_i \text{ mod } p = q[\langle p^i \rangle]$  をそれぞれ求めるステップと、

$0 \leq i < j \leq m-1$  で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$  をそれぞれ求めて、 $0 \leq t \leq k'-1$  で  $q[\langle p^i$

40

50

$(p^i K[t])>$ にMをそれぞれ足し込むとともに、 $q[\langle p^i - (p^i K[t])>]$ にMをそれぞれ足し込むステップと

を有することにも特徴を有し、

第3のステップが、

$0 \leq i \leq m-1$ で、かつ  $1 \leq t \leq k'-1$ で、 $q[\langle p^i \rangle]$ に $q[\langle (p^i K[t])>]$ をそれぞれ足し込むとともに、 $q[\langle p^i \rangle]$ に $q[\langle -(p^i K[t])>]$ をそれぞれ足し込むステップと、

$0 \leq i \leq m-1$ で、 $-q[\langle p^i \rangle] = c_i$ をそれぞれ求めるステップと

を有することにも特徴を有するものである。

【0021】

また、本発明の暗号化/復号化装置では、素数pを標数とし、拡大次数mの拡大体 $F_p^m$ の2つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$ を、平文データと暗号化鍵、または暗号データと復号化鍵として、平文データと暗号化鍵とを乗算させて元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$ を生成することにより暗号化する、または暗号データと復号化鍵とを乗算させて元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$ を生成することにより復号化する演算器を備えた暗号化/復号化装置において、元をそれぞれ記憶する第1の記憶部と、拡大次数mを記憶する第2の記憶部と、 $km+1$ が素数であって、 $F_{km+1}$ でpが原始元となる正整数kを演算器による演算に基づいて特定して記憶する第3の記憶部と、2つの元A、Bを、正整数kを用いて素数pを標数とする拡大次数kmの拡大体 $F_p^{km}$ における2つの元として演算器で乗算した結果を記憶する第4の記憶部と、拡大次数kmの拡大体 $F_p^{km}$ の元の乗算結果を用いて演算器で所定の演算を行って、部分体である拡大次数mの拡大体 $F_p^m$ の元における乗算の結果を求めて記憶する第5の記憶部とを有することとした。

【0022】

さらに、本発明の暗号化/復号化装置では、

$0 \leq i \leq m-1$ 、 $0 \leq j \leq k-1$ とし、

$\langle x \rangle$ がxのmod(km+1)をとるものとして、

第4の記憶部が、

$0 \leq t \leq k-1$ で、 $\langle p^{mt} \rangle = K[t]$ となる各 $K[t]$ をそれぞれ求めて記憶する記憶部と、

$0 \leq i \leq km$ で、それぞれ  $0 = q[\langle i \rangle]$ として記憶する記憶部と、

$0 \leq i \leq m-1$ で、 $a_i b_i \text{ mod } p = q[\langle p^i \rangle]$ をそれぞれ求めて記憶する記憶部と、

$0 \leq i < j \leq m-1$ で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$ をそれぞれ求めて記憶する記憶部と、

$0 \leq t \leq k-1$ で $q[\langle p^i + (p^i K[t])>]$ にMをそれぞれ足し込んで記憶する記憶部と

を有することにも特徴を有し、

第5の記憶部が、

$0 \leq i \leq m-1$ で、かつ  $1 \leq t \leq k-1$ で、 $q[\langle p^i \rangle]$ に $q[\langle (p^i K[t])>]$ をそれぞれ足し込んで記憶する記憶部と、

$0 \leq i \leq m-1$ で、 $kq[\langle 0 \rangle] - q[\langle p^i \rangle] = c_i$ をそれぞれ求めて記憶する記憶部と

を有することにも特徴を有するものである。

【0023】

さらに、本発明の暗号化/復号化装置では、

$k=2k'$ の場合に、

$F_{2k'm+1}$ でpが原始元あるいは位数が $k'm$ かつ $k'm$ が奇数となる正整数 $k'$ として、この正整数 $k'$ を記憶する記憶部を有し、

$0 \leq i \leq m-1$ 、 $0 \leq j \leq 2k'-1$ とし、

$\langle x \rangle$ がxのmod( $2k'm+1$ )をとるものとして、

第4の記憶部が、

$0 \leq t \leq k'-1$ で、 $\langle p^{mt} \rangle = K[t]$ となる各 $K[t]$ をそれぞれ求めて記憶する記憶部と、

$0 \leq i \leq 2k'm$ で、それぞれ  $0 = q[\langle i \rangle]$ として記憶する記憶部と、

$0 \leq i \leq m-1$ で、 $a_i b_i \text{ mod } p = q[\langle p^i \rangle]$ をそれぞれ求めて記憶する記憶部と、

$0 \leq i < j \leq m-1$ で、 $(a_i - a_j)(b_i - b_j) \text{ mod } p = M$ をそれぞれ求めて記憶する記憶部と、

$0 \leq t \leq k'-1$ で $q[\langle p^i + (p^i K[t])>]$ にMをそれぞれ足し込んで記憶するとともに、 $q[$

$\langle p^i - (p^i K[t]) \rangle$ にMをそれぞれ足し込んで記憶する記憶部とを有することにも特徴を有し、

第5の記憶部が、

$0 \leq i \leq m-1$ で、かつ  $1 \leq t \leq k'-1$ で、 $q[\langle p^i \rangle]$ に $q[\langle (p^i K[t]) \rangle]$ をそれぞれ足し込むとともに、 $q[\langle p^i \rangle]$ に $q[\langle -(p^i K[t]) \rangle]$ をそれぞれ足し込んで記憶する記憶部と、

$0 \leq i \leq m-1$ で、 $-q[\langle p^i \rangle] = c_i$ をそれぞれ求めて記憶する記憶部と

を有することにも特徴を有するものである。

【0024】

また、本発明の乗算装置では、素数pを標数とし、拡大次数mの拡大体 $F_p^m$ の2つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$ を乗算して元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$ を生成する演算器を備えた拡大体の乗算装置において、元をそれぞれ記憶する第1の記憶部と、拡大次数mを記憶する第2の記憶部と、 $k+1$ が素数であって、 $F_{k+1}$ でpが原始元となる正整数kを演算器による演算に基づいて特定して記憶する第3の記憶部と、2つの元A, Bを、正整数kを用いて素数pを標数とする拡大次数kmの拡大体 $F_p^{km}$ における2つの元として演算器で乗算した結果を記憶する第4の記憶部と、拡大次数kmの拡大体 $F_p^{km}$ の元の乗算結果を用いて演算器で所定の演算を行って、部分体である拡大次数mの拡大体 $F_p^m$ の元における乗算の結果を求めて記憶する第5の記憶部とを有することとした。

【発明の効果】

【0025】

本発明では、素数pを標数とし、拡大次数mの拡大体 $F_p^m$ の2つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$ を乗算して元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$ を生成する際に、 $k+1$ が素数であって、 $F_{k+1}$ でpが原始元となる正整数kを用いて、素数pを標数とする拡大次数kmの拡大体 $F_p^{km}$ を定義体として想定して演算を行うことにより、拡大次数mを任意の整数とすることができる。

【0026】

すなわち、任意の拡大次数mを用いても、 $k+1$ が素数であって、 $F_{k+1}$ でpが原始元となる正整数kを用いた拡大次数kmの拡大体によって、演算に必要な拡大体を極めて容易に準備できるので、拡大次数mごとに対応した拡大体を準備する必要がなく、拡大次数mを無制限に選択することができる。

【0027】

この拡大次数mは、暗号化及び復号化における鍵長であって、鍵長を任意に選択することができるので、必要に応じて暗号データの安全性を任意に選択可能とすることができる。特に、安全性を高めたい場合は拡大次数mをできるだけ大きくするだけでよく、暗号データの解読行為に対して極めて容易に対応できる。

【0028】

しかも、拡大次数kmの拡大体を定義体として用いることにより、乗算を、所定の元の加算または減算と、乗算との繰り返しに分解して演算することができ、並列処理化が容易であって、高速演算を可能とすることができる。

【0029】

さらに、 $k = 2k'$ となる $k'$ を用いた場合には、所定の元の加算または減算と、乗算との繰り返し回数を削減できることにより、演算のさらなる高速化を図ることができる。

【図面の簡単な説明】

【0030】

【図1】本発明に係る暗号化/復号化装置のブロック図である。

【図2】本発明に係る暗号化/復号化プログラムにおけるフローチャートである。

【図3】本発明に係る暗号化/復号化プログラムにおけるフローチャートである。

【図4】他の実施形態のフローチャートである。

【図5】既約多項式を求めるフローチャートである。

【符号の説明】

10

20

30

40

50



## 【 0 0 3 1 】

- 10 演算器
- 20 不揮発性記憶部
- 30 揮発性記憶部
- 40 データ入出力部
- 50 データバス

## 【 発明を実施するための最良の形態 】

## 【 0 0 3 2 】

本発明の暗号化 / 復号化プログラム、暗号化 / 復号化装置、及び拡大体の乗算装置では、素数  $p$  を標数とする拡大体を定義体とし、拡大次数  $m$  の拡大体  $F_p^m$  の 2 つの元  $A = \{a_0, a_1, a_2, \dots, a_{m-1}\}$ 、 $B = \{b_0, b_1, b_2, \dots, b_{m-1}\}$  を乗算して元  $C = \{c_0, c_1, c_2, \dots, c_{m-1}\}$  を生成する際に、拡大次数  $m$  に対応し、 $km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を用いて素数  $p$  を標数とする拡大次数  $km$  の拡大体  $F_p^{km}$  を新たな定義体として乗算を行い、この乗算の結果を用いて部分体である拡大次数  $m$  の拡大体  $F_p^m$  の元における乗算の結果を求めている。

10

## 【 0 0 3 3 】

すなわち、任意の拡大次数  $m$  に対応して、 $km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる正整数  $k$  を用いることにより、素数  $p$  を標数とする拡大次数  $m$  の拡大体  $F_p^m$  を部分体とする拡大次数  $km$  の拡大体  $F_p^{km}$  を定義体として用いることができ、拡大次数  $m$  及び標数  $p$  を任意としても 2 つの元  $A$ 、 $B$  の乗算を行うことができる。

20

## 【 0 0 3 4 】

ここで、拡大次数  $m$  は、暗号化及び復号化における鍵長に当たり、任意の拡大次数  $m$  が選択できるということは、鍵長を任意に選択できることを示しており、必要に応じて適宜の鍵長として暗号データを生成することができる。

## 【 0 0 3 5 】

したがって、状況に応じて鍵長を選択することにより、暗号データの安全性と、暗号化及び復号化の演算の負荷をバランスさせながら適宜の鍵長とした暗号データを生成できる。

## 【 0 0 3 6 】

例えば、標数  $p = 2^{500} - 863$  の 500 ビットの素数を用いた場合には、下表に示すように、拡大次数  $m$ 、パラメータとなる正整数  $k$ 、鍵長の組み合わせを選択できる。

30

## 【 表 1 】

拡大次数 $m$	2	3	4	5	...
パラメータ $k$	1	2	1	2	...
鍵長 (ビット)	1000	1500	2000	2500	...

## 【 0 0 3 7 】

ここで、鍵長が短くなる組み合わせを用いれば、暗号化及び復号化の演算速度を向上させることができ、鍵長が長くなる組み合わせを用いれば、解読困難な暗号化データを生成して安全性を向上させることができる。

40

## 【 0 0 3 8 】

特に、拡大次数  $m$  は、任意な正整数とすることができ、いくらでも大きくすることもできる。また、標数  $p$  も任意の素数とすることができ。

## 【 0 0 3 9 】

なお、暗号化に必要な鍵は、Diffie - Hellman 鍵交換アルゴリズムを用いて受け渡すことにより、安全に受け渡すことができる。

## 【 0 0 4 0 】

50

すなわち、アリスとボブが鍵交換を行う場合、まず、アリスからボブに鍵データとして  $g$  ,  $A = g^a \quad F_p^m$  を送信している。

【0041】

ボブは、 $A$  を受信すると、 $C = A^b = g^{ab} \quad F_p^m$  を計算して、 $B = g^b \quad F_p^m$  を計算し、 $B = g^b$  をアリスに送信している。

【0042】

アリスは、 $B$  を受信して  $C = B^a = g^{ab} \quad F_p^m$  を計算することにより、アリスとボブとを接続するネットワーク上に鍵  $g^{ab}$  を流すことなく共有することができる。

【0043】

なお、ICカードにおける認証用データに用いる鍵の場合には、ICカードの作成時にあらかじめICカードに鍵データを記憶させておくことにより、ネットワーク上に鍵を流すことなく共有することができる。

【0044】

あるいは、一般的な公開鍵暗号の場合であれば、ボブがアリスから所要のデータを受け取る際に、ボブは予め公開鍵を公開しておく。

【0045】

例えば、Elgamal暗号の場合であれば、ボブは秘密鍵  $s$  を用いて、 $g$  ,  $B = g^s \quad F_p^m$  を計算して公開しておく。

【0046】

メッセージ  $M$  を送信するアリスは、ボブの公開鍵データ  $g$  ,  $B$  をダウンロードして、メッセージ  $M$  に対して、

$$C_1 = M \times B^t, \quad C_2 = g^t$$

を計算することにより暗号化を行っている。ここで、 $t$  は乱数である。

【0047】

また、 $C_1$  の演算を行うに当たり、後述する本発明の暗号化 / 復号化プログラム、暗号化 / 復号化装置、あるいは拡大体の乗算装置を用いている。

【0048】

アリスは、 $C_1$ 、 $C_2$  をボブに送信し、ボブは、受信した  $C_1$ 、 $C_2$  を用いて、 $C_1 / C_2^s$  を演算することによりメッセージ  $M$  の復号化を行っている。すなわち、

$$C_1 / C_2^s = M B^t / g^{ts} = M g^{ts} / g^{ts}.$$

【0049】

この復号化においても、後述する本発明の暗号化 / 復号化プログラム、暗号化 / 復号化装置、あるいは拡大体の乗算装置を用いている。

【0050】

このようにメッセージ  $M$  の復号化は、 $s$  を秘密にもつボブのみが行える計算であり、対称鍵暗号のようにある一つのパスワードを互いに共有する必要がなく、かつ安全性が確保される長さの鍵を使用することで高い信頼性を有することができる。

【0051】

図1は、本実施形態の暗号化 / 復号化装置のブロック図である。なお、この暗号化 / 復号化装置は拡大体の乗算装置でもある。

【0052】

暗号化 / 復号化装置は、CPU (中央演算装置) などの演算器10と、この演算器10が実行するプログラムなどを記憶した不揮発性記憶部20と、プログラムの実行にともなって必要となるデータを一時的に格納する揮発性記憶部30とを備えている。不揮発性記憶部20は、いわゆるROM (Read Only Memory) あるいはハードディスクなどの不揮発性の記憶手段で構成し、揮発性記憶部30はいわゆるRAM (Random Access Memory) で構成している。

【0053】

特に、揮発性記憶部30は、複数のレジスタを備えており、それぞれのレジスタで所要のデータを記憶している。

10

20

30

40

50

## 【 0 0 5 4 】

不揮発性記憶部20には、本実施形態の暗号化／復号化プログラムを記憶しており、この暗号化／復号化プログラムを起動させることにより、必要に応じて暗号化／復号化プログラムを揮発性記憶部30に展開して、暗号化あるいは復号化の演算を行っている。

## 【 0 0 5 5 】

さらに、暗号化／復号化装置にはデータ入出力部40を設けており、このデータ入力部40を介して任意の拡大次数  $m$  の値を入力可能とし、入力された拡大次数  $m$  の値に基づいて暗号化を実行可能としている。あるいは、拡大次数  $m$  の値だけでなく、標数  $p$  の値を変更可能とすることもできる。

## 【 0 0 5 6 】

また、データ入出力部40では、公開鍵となる鍵データの出力や、暗号化されたデータの入出力などを行っている。図1中、50はデータバスである。

## 【 0 0 5 7 】

演算器10では、必要に応じて、揮発性記憶部30に記憶されている所要の鍵データ、標数  $p$  の値、拡大次数  $m$  などを不揮発性記憶部20に記憶させてもよい。

## 【 0 0 5 8 】

暗号化／復号化装置あるいは拡大体の乗算装置は、このように暗号化／復号化プログラムを実行する電子計算機などの装置に限定するものではなく、暗号化／復号化プログラムに相当する演算を実行する演算回路を備えた演算用デバイスとして、演算処理の高速化を図ることもできる。

## 【 0 0 5 9 】

以下において、暗号化あるいは復号化における2つの元の乗算について説明する。

## 【 0 0 6 0 】

まず、第1実施形態として、以下の条件下における元  $A$  と元  $B$  の積の演算について説明する。ここで、この積の演算が暗号化である場合には、元  $A$  と元  $B$  のいずれか一方が暗号化鍵であって、他方が暗号化鍵の鍵長ごとに分断された単位長平文データであり、積の演算が復号化である場合には、元  $A$  と元  $B$  のいずれか一方が復号化鍵であって、他方が復号化鍵の鍵長ごとに分断された単位長暗号データである。

## 【 0 0 6 1 】

- ・素数  $p$  を標数とする拡大体を定義体とする。
- ・拡大次数  $m$  に対し、 $km+1$  が素数であって、 $F_{km+1}$  で  $p$  が原始元となる適当な正整数  $k$ 。
- ・  $0 \leq i \leq m-1$ 、 $0 \leq j \leq k-1$ 。
- ・  $\langle x \rangle$  が  $x$  の  $\text{mod}(km+1)$  をとるものとする。
- ・  $\omega$  を1の原始  $km+1$  乗根とする。
- ・  $\{a_0, a_1, a_2, \dots, a_{m-1}\}$  を拡大次数  $m$  の拡大体  $F_p^m$  の元  $A$

## 【 数 1 】

$$A = \sum_{i=0}^{m-1} a_i \left( \sum_{j=0}^{k-1} \omega^{\langle p^{i+mj} \rangle} \right) = \sum_{i=0}^{m-1} a_i \gamma^{p^i}, \gamma = \sum_{j=0}^{k-1} \omega^{\langle p^{mj} \rangle}$$

- ・  $\{b_0, b_1, b_2, \dots, b_{m-1}\}$  を拡大次数  $m$  の拡大体  $F_p^m$  の元  $B$

## 【 数 2 】

$$B = \sum_{i=0}^{m-1} b_i \left( \sum_{j=0}^{k-1} \omega^{\langle p^{i+mj} \rangle} \right) = \sum_{i=0}^{m-1} b_i \gamma^{p^i}$$

## 【 0 0 6 2 】

なお、任意の正整数  $m$  に対して、 $km+1$  が素数となる正整数  $k$  が少なくとも  $k < m$  の範囲に存在していることは一般的に証明済みの事実であり、正整数  $k$  を特定する専用プログラムを用いて容易に見つけ出すことができる。

10

20

30

40

50

## 【 0 0 6 3 】

通常、元 A と元 B の積  $C = A B$  は、C V M A (Cyclic Vector Multiplication Algorithm) で計算されるが、部分体における演算の閉性から元 A と元 B の積 C も部分体  $F_p^m$  の元なることから、積 C のベクトル表現においても、基底ベクトル  $\omega'$  と  $\omega''$  のベクトル係数が等しくなる。

## 【 0 0 6 4 】

ここで、表記の便宜上、

## 【 数 3 】

$$\omega' = \omega \langle p^i \rangle$$

10

及び、

## 【 数 4 】

$$\omega'' = \omega \langle p^{i+m_j} \rangle$$

である。

## 【 0 0 6 5 】

したがって、求める必要があるのは  $0 \leq i \leq m-1$  での  $\omega'$  の各係数  $c_i$  のみであり、

## 【 数 5 】

$$C = \sum_{i=0}^{m-1} c_i \left( \sum_{j=0}^{k-1} \omega \langle p^{i+m_j} \rangle \right) = \sum_{i=0}^{m-1} c_i \gamma^{p^i}$$

20

として、係数  $c_i$  は、図 2 に示すフローチャートに基づく暗号化 / 復号化プログラムにより、パーソナルコンピュータなどの電子計算機での演算によって求めることができる。

## 【 0 0 6 6 】

ただし、この場合、直接、 $8p|m(p-1)$  となる拡大体を構成することはできない。そこで、 $8p|m(p-1)$  となる拡大体を構成する場合には、拡大次数  $m$  の偶数因数部分  $m_E$  と奇数因数部分  $m_O$  とに分けて ( $m = m_E \cdot m_O$ )、それぞれを逐次拡大体に分けて拡大することにより、 $8p|m(p-1)$  となる拡大体にも対応可能とすることができる。なお、場合によっては後述する第 2 実施形態を組み合わせる用いることが必要となることもある。

30

## 【 0 0 6 7 】

暗号化の場合には、まず、電子計算機では拡大次数  $m$  を設定する (ステップ S 1)。なお、復号化の場合には、電子計算機は、秘密鍵または公開鍵の鍵長から拡大次数  $m$  を特定することもできる。

## 【 0 0 6 8 】

次いで、電子計算機は、設定された拡大次数  $m$  に基づいて、 $km+1$  が素数であって、 $F_{k m+1}$  で  $p$  が原始元となる適当な正整数  $k$  を専用プログラムを用いて特定する (ステップ S 2)。なお、前述したように、 $k < m$  の範囲で  $km+1$  が素数となる正整数  $k$  は少なくとも 1 つは特定でき、電子計算機は、比較的短時間で正整数  $k$  の特定処理を終了することができる。

40

## 【 0 0 6 9 】

次いで、電子計算機は、 $0 \leq t \leq k-1$  で、 $\langle p^{m^t} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求め (ステップ S 3)、さらに、 $0 \leq i \leq km$  で、それぞれ  $0 = q[\langle i \rangle]$  とする (ステップ S 4)。

## 【 0 0 7 0 】

次いで、電子計算機は、 $0 \leq i \leq m-1$  で、 $a_i b_i \bmod p = q[\langle p^i \rangle]$  をそれぞれ求め (ステップ S 5)、その後、 $0 \leq i < j \leq m-1$  で、 $(a_i - a_j)(b_i - b_j) \bmod p = M$  をそれぞれ求めて、 $0 \leq t \leq k-1$  で  $q[\langle p^i + (p^j K[t]) \rangle]$  への  $M$  の足し込みをそれぞれ行う (ステップ S 6)。

## 【 0 0 7 1 】

その後、電子計算機は、拡大次数  $m$  の拡大体  $F_p^m$  ではなく、拡大次数  $km$  の拡大体を定義

50

体として用いていることによる処理として、 $0 \leq i \leq m-1$ で、かつ  $1 \leq t \leq k-1$ で、 $q[\langle p^i \rangle]$ への $q[\langle (p^i K[t]) \rangle]$ の足し込みをそれぞれ行って（ステップS7）、最後に、 $0 \leq i \leq m-1$ で、 $kq[\langle 0 \rangle] - q[\langle p^i \rangle] = c_i$ を求めている（ステップS8）。

#### 【0072】

このように、 $c_i$ は、拡大次数 $km$ の拡大体 $F_p^{km}$ における所定の元の加算または減算と、乗算との繰り返しに分解して演算を行うことができ、並列処理化が容易であって、高速演算を可能とすることができる。

#### 【0073】

特に、演算の負荷が小さいことにより、携帯電話機やICカードなどの演算機能の乏しい装置でも容易に乗算処理を実行でき、しかも公開鍵及び秘密鍵の鍵長の変更を可能とすることができる。

10

#### 【0074】

さらに、乗算処理における演算は、演算処理回路として半導体基板上に形成して乗算処理用半導体デバイスとすることもでき、この乗算処理用半導体デバイスを備えた暗号化/復号化装置として、暗号化及び復号化のさらなる高速化を図ることができ、しかも、並列処理化が可能であって、一層の高速化を図ることができる。また、拡大体の乗算装置として乗算処理用半導体デバイスを用いることもできる。

#### 【0075】

すなわち、乗算処理用半導体デバイスでは、半導体基板上に、所要の演算を実行可能とした演算器を形成するとともに、各記憶部として以下のレジスタ及びレジスタ群を形成している。

20

- ・ 標数  $p$  を記憶するレジスタ。
- ・ 拡大次数  $m$  を記憶するレジスタ。
- ・ 拡大次数  $m$  に基づく拡大体  $F_p^m$  の元  $A$  を記憶するレジスタ群。
- ・ 拡大次数  $m$  に基づく拡大体  $F_p^m$  の元  $B$  を記憶するレジスタ群。
- ・ 設定された拡大次数  $m$  に対応した正整数  $k$  を特定して記憶するレジスタ。
- ・  $0 \leq t \leq k-1$  で、 $\langle p^m \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めて記憶するレジスタ群。
- ・  $0 \leq i \leq km-1$  で、それぞれ  $0 = q[\langle i \rangle]$  として記憶するレジスタ群。
- ・  $0 \leq i \leq m-1$  で、 $a_i b_i \bmod p = q[\langle p^i \rangle]$  をそれぞれ求めて記憶するレジスタ群。
- ・  $0 \leq i < j \leq m-1$  で、 $(a_i - a_j)(b_i - b_j) \bmod p = M$  をそれぞれ求めて記憶するレジスタ群。
- ・  $0 \leq t \leq k-1$  で  $q[\langle p^i + (p^i K[t]) \rangle]$  に  $M$  をそれぞれ足し込んで記憶するレジスタ群。
- ・  $0 \leq i \leq m-1$  で、かつ  $1 \leq t \leq k-1$  で、 $q[\langle p^i \rangle]$  に  $q[\langle (p^i K[t]) \rangle]$  をそれぞれ足し込んで記憶するレジスタ群。
- ・  $0 \leq i \leq m-1$  で、 $kq[\langle 0 \rangle] - q[\langle p^i \rangle] = c_i$  をそれぞれ求めて記憶するレジスタ群。

30

#### 【0076】

これらのレジスタ及びレジスタ群を設けることにより、各演算は並列化が可能であるので、並列処理を行うことにより乗算処理をさらに高速化することができる。したがって、高速な暗号化及び復号化を可能とする暗号化/復号化装置、あるいは拡大体の乗算装置を提供できる。

#### 【0077】

この乗算処理用半導体デバイスを所要の実装ボードに装着することにより、高速な乗算処理を可能とする実装ボードを提供でき、この実装ボードを用いて携帯電話機や電子計算機などを構成することにより、高速な暗号化及び復号化が可能であって、しかも公開鍵及び秘密鍵の鍵長の長さを自在に可変とした携帯電話機や電子計算機などを提供することができる。

40

#### 【0078】

以下において、第2実施形態として、以下の条件下における元  $A$  と元  $B$  の積の演算について説明する。ここで、第1実施形態との違いは、 $k = 2k'$  となる  $k'$  を用いて演算を行うことである。すなわち、

- ・ 素数  $p$  を標数とする拡大体を定義体とする。

50

・拡大次数  $m$  に対し、 $2k'm+1$  が素数であって、 $F_{2k'm+1}$  で  $p$  が原始元あるいは位数が  $k'm$  かつ  $k'm$  が奇数となる適当な正整数  $k'$ 。

・  $0 \leq i \leq m-1, 0 \leq j \leq 2k'-1$ 。

・  $\langle x \rangle$  が  $x$  の  $\text{mod}(2k'm+1)$  をとるものとする。

・  $\omega$  を 1 の原始  $2k'm+1$  乗根として、 $\omega = \omega^{+1}$  とする。

・  $\{a_0, a_1, a_2, \dots, a_{m-1}\}$  を拡大次数  $m$  の拡大体  $F_p^m$  の元  $A$

【数 6】

$$A = \sum_{i=0}^{m-1} a_i \left( \sum_{j=0}^{k'-1} \tau^{\langle p^{i+mj} \rangle} \right) = \sum_{i=0}^{m-1} a_i \gamma^{p^i}, \gamma = \sum_{j=0}^{k'-1} \tau^{\langle p^{mj} \rangle}$$

10

・  $\{b_0, b_1, b_2, \dots, b_{m-1}\}$  を拡大次数  $m$  の拡大体  $F_p^m$  の元  $B$

【数 7】

$$B = \sum_{i=0}^{m-1} b_i \left( \sum_{j=0}^{k'-1} \tau^{\langle p^{i+mj} \rangle} \right) = \sum_{i=0}^{m-1} b_i \gamma^{p^i}$$

【0079】

部分体における演算の閉性から元  $A$  と元  $B$  の積  $C$  も部分体  $F_p^m$  の元なることから、積  $C$  のベクトル表現においても、基底ベクトル  $\tau^{\langle p^i \rangle}$  と  $\tau^{\langle p^{i+mj} \rangle}$  のベクトル係数が等しくなる。

20

【0080】

ここで、表記の便宜上、

【数 8】

$$\tau' = \tau^{\langle p^i \rangle}$$

及び、

【数 9】

$$\tau'' = \tau^{\langle p^{i+mj} \rangle}$$

である。

30

【0081】

したがって、求める必要があるのは  $0 \leq i \leq m-1$  での  $\tau^{\langle p^i \rangle}$  の係数  $c_i$  のみであり、

【数 10】

$$C = \sum_{i=0}^{m-1} c_i \left( \sum_{j=0}^{k'-1} \tau^{\langle p^{i+mj} \rangle} \right) = \sum_{i=0}^{m-1} c_i \gamma^{p^i}$$

として、係数  $c_i$  は、図 3 に示すフローチャートに基づくプログラムにより、パーソナルコンピュータなどの電子計算機での演算によって求めることができる。

【0082】

40

ただし、この場合には、 $4p|m(p-1)$  となる拡大体を構成することはできない。そこで、 $4p|m(p-1)$  となる拡大体を構成する場合には、拡大次数  $m$  の偶数因数部分  $m_E$  と奇数因数部分  $m_O$  とに分けて ( $m = m_E \cdot m_O$ )、それぞれを逐次拡大体に分けて拡大することにより、 $4p|m(p-1)$  となる拡大体にも対応可能とすることができる。なお、場合によっては前述した第 1 実施形態を組み合わせる必要があることもある。

【0083】

暗号化の場合には、まず、電子計算機では拡大次数  $m$  を設定する (ステップ T1)。なお、復号化の場合には、電子計算機は、秘密鍵または公開鍵の鍵長から拡大次数  $m$  を特定する。

【0084】

50

次いで、電子計算機は、設定された拡大次数  $m$  に基づいて、 $2k'm+1$  が素数であって、 $F_{2k'm+1}$  で  $p$  が原始元あるいは位数が  $k'm$  かつ  $k'm$  が奇数となる適当な正整数  $k'$  を専用プログラムを用いて特定する（ステップ T2）。なお、前述したように、 $2k' < m$  の範囲で  $2k'm+1$  が素数となる正整数  $k'$  は少なくとも 1 つは特定でき、電子計算機は、比較的短時間で正整数  $k'$  の特定処理を終了することができる。

【0085】

次いで、電子計算機は、 $0 \leq t < k'-1$  で、 $\langle p^{m^t} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求め（ステップ T3）、さらに、 $0 \leq i < 2k'm$  で、それぞれ  $0 = q[\langle i \rangle]$  とする（ステップ T4）。

【0086】

次いで、電子計算機は、 $0 \leq i < m-1$  で、 $a_i, b_i \bmod p = q[\langle p^i \rangle]$  をそれぞれ求め（ステップ T5）、その後、 $0 \leq i < j < m-1$  で、 $(a_i - a_j)(b_i - b_j) \bmod p = M$  をそれぞれ求めて、 $0 \leq t < k'-1$  で  $q[\langle p^i + (p^j K[t]) \rangle]$  への  $M$  の足し込みをそれぞれ行うとともに、 $q[\langle p^i - (p^j K[t]) \rangle]$  への  $M$  の足し込みをそれぞれ行う（ステップ T6）。

10

【0087】

その後、電子計算機は、拡大次数  $m$  の拡大体  $F_p^m$  ではなく、拡大次数  $k'm$  の拡大体を定義体として用いていることによる処理として、 $0 \leq i < m-1$  で、かつ  $1 \leq t < k-1$  で、 $q[\langle p^i \rangle]$  への  $q[\langle (p^i K[t]) \rangle]$  の足し込みをそれぞれ行うとともに、 $q[\langle p^i \rangle]$  への  $q[\langle -(p^i K[t]) \rangle]$  の足し込みをそれぞれ行って（ステップ T7）、電子計算機は、最後に、 $0 \leq i < m-1$  で、 $-q[\langle p^i \rangle] = c_i$  を求めている（ステップ T8）。

20

【0088】

このように、 $c_i$  は、所定の元の加算または減算と、乗算との繰り返しに分解して演算を行うことができ、並列処理化が容易であって、高速演算を可能とすることができる。

【0089】

また、図3に示したフローチャートの乗算処理の演算も、演算処理回路として半導体基板上に形成して乗算処理用半導体デバイスとすることもでき、この乗算処理用半導体デバイスを備えた暗号化/復号化装置として、暗号化及び復号化のさらなる高速化を図ることができ、しかも、並列処理化が可能であって、一層の高速化を図ることができる。また、拡大体の乗算装置として乗算処理用半導体デバイスを用いることもできる。

【0090】

この場合、乗算処理用半導体デバイスでは、半導体基板上に、所要の演算を実行可能とした演算器を形成するとともに、各記憶部として以下のレジスタ及びレジスタ群を形成している。

30

- ・ 標数  $p$  を記憶するレジスタ。
- ・ 拡大次数  $m$  を記憶するレジスタ。
- ・ 拡大次数  $m$  に基づく拡大体  $F_p^m$  の元  $A$  を記憶するレジスタ群。
- ・ 拡大次数  $m$  に基づく拡大体  $F_p^m$  の元  $B$  を記憶するレジスタ群。
- ・ 設定された拡大次数  $m$  に対応した正整数  $k'$  を特定して記憶するレジスタ。
- ・  $0 \leq t < k'-1$  で、 $\langle p^{m^t} \rangle = K[t]$  となる各  $K[t]$  をそれぞれ求めて記憶するレジスタ群。
- ・  $0 \leq i < 2k'm-1$  で、それぞれ  $0 = q[\langle i \rangle]$  として記憶するレジスタ群。
- ・  $0 \leq i < m-1$  で、 $a_i, b_i \bmod p = q[\langle p^i \rangle]$  をそれぞれ求めて記憶するレジスタ群。
- ・  $0 \leq i < j < m-1$  で、 $(a_i - a_j)(b_i - b_j) \bmod p = M$  をそれぞれ求めて記憶するレジスタ群。
- ・  $0 \leq t < k'-1$  で  $q[\langle p^i + (p^j K[t]) \rangle]$  に  $M$  をそれぞれ足し込んで記憶するとともに、 $q[\langle p^i - (p^j K[t]) \rangle]$  に  $M$  をそれぞれ足し込んで記憶するレジスタ群。
- ・  $0 \leq i < m-1$  で、かつ  $1 \leq t < k'-1$  で、 $q[\langle p^i \rangle]$  に  $q[\langle (p^i K[t]) \rangle]$  をそれぞれ足し込んで記憶するとともに、さらに、 $q[\langle p^i \rangle]$  に  $q[\langle -(p^i K[t]) \rangle]$  をそれぞれ足し込んで記憶するレジスタ群。
- ・  $0 \leq i < m-1$  で、 $-q[\langle p^i \rangle] = c_i$  をそれぞれ求めて記憶するレジスタ群。

40

【0091】

これらのレジスタ及びレジスタ群を設けることにより、第1の実施形態の場合と同様に

50

、各演算は並列化が可能であるので、並列処理を行うことにより乗算処理をさらに高速化することができる。したがって、高速な暗号化及び復号化を可能とする暗号化/復号化装置、あるいは拡大体の乗算装置を提供できる。

【0092】

さらに、 $km+1$ を素数とし、 $S$ をmod  $km+1$ における位数  $k$  の部分巡回乗法群として、 $km$ 次のAOP (All One Polynomial)  $(x^{km+1} - 1) / (x - 1)$ の零点を  $\gamma$ として、

【数11】

$$\gamma = \sum_{a \in S} \omega^a$$

10

で与えられる  $\gamma$  を用い、次の集合を考える。

【数12】

$$\{\gamma, \gamma^p, \dots, \gamma^{p^{m-1}}\}$$

【0093】

【数12】の集合が拡大体 $F_p^m$ において正規基底を成すことは、 $km/e$ が $m$ と互いに素となることと必要十分である。ここで、 $e$ は $p$ のmod  $km+1$ での位数である。前述した第1実施形態及び第2実施形態は、この正規基底を用いた乗算に適用可能となっている。

【0094】

20

すなわち、

- ・  $e$ を $F_{km+1}$ における元 $p$ の位数とする。
- ・  $e' = km / e$
- ・ 1の原始 $k$ 乗根  $\omega \in F_{km+1}$ とする。
- ・  $\{a_0, a_1, a_2, \dots, a_{m-1}\}$ を拡大次数 $m$ の拡大体 $F_p^m$ の元 $A$

【数13】

$$A = \sum_{i=0}^{m-1} a_i \gamma^{p^i}$$

30

- ・  $\{b_0, b_1, b_2, \dots, b_{m-1}\}$ を拡大次数 $m$ の拡大体 $F_p^m$ の元 $B$

【数14】

$$B = \sum_{i=0}^{m-1} b_i \gamma^{p^i}$$

【0095】

このとき、部分体における演算の閉性から元 $A$ と元 $B$ の積 $C$ は、

【数15】

$$C = AB = \sum_{i=0}^{m-1} c_i \gamma^{p^i}$$

40

として、係数 $c_i$ は、図4に示すフローチャートに基づくプログラムにより、パーソナルコンピュータなどの電子計算機での演算によって求めることができる。

【0096】

ここで、暗号化の場合には、まず、電子計算機では拡大次数 $m$ を設定する(ステップU1)。なお、復号化の場合には、電子計算機は、秘密鍵または公開鍵の鍵長から拡大次数 $m$ を特定する。

【0097】

次いで、電子計算機は、設定された拡大次数 $m$ に基づいて、 $km+1$ が素数であって、 $e'$

50



( $= km/e$ )と $m$ とが互いに素となる適当な正整数 $k$ を専用プログラムを用いて特定する(ステップU2)。正整数 $k$ の特定にともなって、1の原始 $k$ 乗根の を特定する(ステップU3)。

【0098】

次いで、電子計算機は、 $1 = K[0]$ 、 $0 = r[0]$ とする(ステップU4)。

【0099】

次いで、電子計算機は、 $0 \leq i < m$ で、 $0 = q[i]$ とする(ステップU5)。

【0100】

次いで、電子計算機は、 $1 \leq t < k-1$ で、 $\langle K[t-1] \rangle = K[t]$ とする(ステップU6)。

【0101】

次いで、電子計算機は、 $0 \leq t < m-1$ であって、 $0 \leq t < k-1$ で、 $i+1 = r[\langle p^i K[t] \rangle]$ とする(ステップU7)。

【0102】

次いで、電子計算機は、 $0 \leq t < m-1$ で、 $a_i b_i \bmod p = q[i+1]$ をそれぞれ求める(ステップU8)。

【0103】

次いで、電子計算機は、 $0 \leq i < j < m-1$ で、 $(a_i - a_j)(b_i - b_j) \bmod p = M$ をそれぞれ求めて、 $0 \leq t < k-1$ で $q[r[\langle p^i + (p^j K[t]) \rangle]]$ への $M$ の足し込みをそれぞれ行う(ステップU9)。

【0104】

最後に、電子計算機は、 $0 \leq i < m-1$ で、 $kq[\langle 0 \rangle] - q[i+1] = c_i$ を求めている(ステップU10)。

【0105】

なお、 $k$ が偶数の場合には、ステップU9において $kq[\langle 0 \rangle] = 0$ とすることができる。

【0106】

このように、より多くの正規基底に対して適用可能とすることができる。しかも、 $k$ の値をより小さくすることができるので、演算回数の削減による演算処理の高速化を図ることもできる。

【0107】

なお、前述したように、 $8p|m(p-1)$ あるいは $4p|m(p-1)$ などのように、 $m$ が $p$ の倍数である場合には拡大体を構成できないことがあるが、拡大次数 $m$ を偶数因数部分 $m_E$ と奇数因数部分 $m_O$ とに分けて、それぞれを逐次拡大体に分けて拡大することにより、奇標数 $p$ に対しての拡大体の構成を可能とすることができ、上記の制限を排除することができる。

【0108】

すなわち、例えば、 $F_p^{4p}$ を構成する場合を考える。この場合には、最初に $F_p^4$ の拡大体を構成し、次いで、この拡大体を $p$ 次逐次拡大することにより、奇標数 $p$ が4と互いに素であることから $F_p^{4p}$ で表される拡大体を構成できる。すなわち、任意の奇標数及び任意次数の拡大体を構成することが可能である。

【0109】

本発明は数学的に見た場合には、既約多項式として法多項式を準備することなく拡大体における乗算や除算を行えるものであり、見方を変えれば本発明の考え方を利用することにより、任意次数の既約多項式を生成することができることを示している。

【0110】

ここで、例えば $F_p^4$ の $(1, 2, 1, 2)$ というベクトル表現を持つ元は $F_p^2$ の元である。真部分体に含まれないような元を真性元と呼ぶこととして、 $F_p^m$ の真性元を とした場合、その最小多項式、すなわち を零点にもつ $F_p$ 上の最小次数の多項式 $M(x)$ が求めれば、それは $F_p$ 上の $m$ 次既約多項式となっている。

【0111】

なお、 $M(x)$ は、次式で表される。

10

20

30

40

【数 1 6】

$$M_{\alpha}(x) = (x - \alpha)(x - \alpha^p) \dots (x - \alpha^{p^{m-1}}) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0,$$

$$a_0, a_1, a_2, \dots, a_{m-1} \in F_p$$

【0 1 1 2】

ここで、次式の計算式を考えることにする。

10

【数 1 7】

$$a_{m-1} = -Tr(\alpha)$$

【数 1 8】

$$a_i = (m-i)^{-1} \left\{ -Tr(\alpha^{m-i}) + \sum_{j=1}^{m-1-i} (-1)^j a_{m-j} Tr(\alpha^{m-i-j}) \right\}$$

20

$$Tr(x) = x + x^p + x^{p^2} + \dots + x^{p^{m-1}}$$

【0 1 1 3】

上式で、 $i = m-2, m-3, \dots, 2, 1, 0$ の順に計算されることにより既約多項式が求められることとなる。

【0 1 1 4】

すなわち、拡大体 $F_p^m$ の任意の真性元  $\alpha$  の最小多項式は、図 5 に示すフローチャートに基づくプログラムにより、下のようにして求めることができる。

【0 1 1 5】

30

まず、電子計算機では、真性元  $\alpha$  のベクトル表現  $(x_0, x_1, x_2, \dots, x_{m-1})$  を設定する (ステップ W 1)。ここで、真性元  $\alpha$  の最小多項式  $M(x)$  は次式となるものとする。

【数 1 9】

$$M_{\alpha}(x) = x^m + \sum_{i=0}^{m-1} a_i x^i$$

【0 1 1 6】

次いで、電子計算機は、 $1 \leq i \leq m$  で、 $T[i] = Tr(\alpha^i)$  とし (ステップ W 2)、 $a[m-1] = -T[1]$  とする (ステップ W 3)。

40

【0 1 1 7】

次いで、電子計算機は、 $m-2 \geq i \geq 0$  で、 $0 = M$  とし、 $0 \leq j \leq m-1-i$  で、 $-a[m-j]Tr(\alpha^{m-i-j})$  の  $M$  への足し込みをそれぞれ行う (ステップ W 4)。

【0 1 1 8】

次いで、電子計算機は、 $a[i] = (m-i)^{-1} \{M - Tr(\alpha^{m-i})\}$  を求めている (ステップ W 5)。

【0 1 1 9】

これにより、 $p > m$  を満たす任意の既約多項式を求めることができる。なお、前述した処理は、素体 $F_p$ ではない部分体に関する最小多項式の特定に用いることもできる。

【0 1 2 0】

このように任意の既約多項式を求めることができることによって、異なる定義体間の基

50

基底変換を可能とすることができる。

【0121】

基底変換を行うためには変換行列を特定する必要があるが、ここで変換行列を生成したい拡大体 $F'_p{}^m$ があり、これと同型の拡大体として $F_p{}^m$ を考える。なお、本明細書においては、数学において通常使用されている「 $\wedge$ 」記号付きの表現が利用できないため、以下においては「 $\wedge$ 」の代わりに「 $'$ 」を代用している。

【0122】

第1実施形態の方法を用いた基底変換行列の生成方法を考える。このとき、パラメータ $k$ によって $(x^{k^{m+1}} - 1)/(x-1)$ という法多項式を考え、その零点を用いて次式で表される $\gamma$ を考え、この $\gamma$ を用いて次式の正規基底を考える。ここで、 $\gamma$ は $F_p{}^{km}$ に真性元として存在する。

10

【数20】

$$\gamma = \sum_{i=0}^{k-1} \omega^{p^{im}}$$

【数21】

$$\{\gamma, \gamma^p, \gamma^{p^2}, \dots, \gamma^{p^{m-1}}\}$$

20

【0123】

この $\gamma$ に相当する元 $\gamma'$ を拡大体 $F'_p{}^m$ の中から見つけることができれば拡大体 $F'_p{}^m$ における正規基底を特定し、基底間での対応関係から変換行列を特定することができる。この変換行列の逆行列を求めれば基底変換を可能とすることができる。

【0124】

ここで、元 $\gamma'$ を求めるためには $\gamma$ に相当する $\gamma'$ を拡大体 $F'_p{}^{km}$ において特定すればよく、 $\gamma$ を拡大体 $F'_p{}^{km}$ において特定するためには拡大体 $F'_p{}^m$ を $k$ 次逐次拡大して $F_p{}^{km}$ と同型の $F'_p{}^{km}$ を構成する。

【0125】

ここで、 $k$ と $m$ が互いに素になるようにして、

30

(1)  $k'k+1$ が素数である。

(2)  $p$ の $F_{k'k+1}$ における位数が $k'k$ である(すなわち原始元である)

ことを満たす $k'$ を求めることができると、 $(x^{k'k+1} - 1)/(x-1)$ を法として、 $F'_p{}^m$ を $k$ 次逐次拡大して $F'_p{}^{mk}$ を構成することができる。ここで、「 $k'$ 」の「 $'$ 」は「 $\wedge$ 」の代用ではない。

【0126】

この逐次拡大体 $F'_p{}^{km}$ から次式を満たす元 $B'$ を探し、 $\gamma'$ を求める。

【数22】

$$B'^{(p^{km}-1)/(km+1)} \neq 1, \omega' = B'^{(p^{km}-1)/(km+1)}$$

40

【0127】

ここで、 $\gamma'$ は位数 $km+1$ の元となるので、 $F_p{}^{km}$ の位数 $km+1$ の元 $\omega'$ に対応することとなる。

【0128】

したがって、次式で与えられる元 $\gamma'$ により以下の集合を考えると、この集合を $F'_p{}^m$ の基底と対応づけることができる。これを用いて変換行列及びその逆行列を求めることができ、基底変換を可能とすることができる。

【数 2 3】

$$\gamma^i = \sum_{i=0}^{k-1} \omega^{ip^{im}}$$

【数 2 4】

$$\{\gamma^1, \gamma^{1p}, \gamma^{1p^2}, \dots, \gamma^{1p^{m-1}}\}$$

【0 1 2 9】

10

このように基底変換が可能なることから、既約多項式の因数分解を可能とすることができる。

【0 1 3 0】

すなわち、まず、 $F_p$ 上の $m$ 次既約多項式 $f(x)$ を考え、その零点 $\alpha$ による多項式基底 $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ を用いて $F_p^m$ を構成することができる。ここで、「 $\alpha$ 」は「 $\wedge$ 」による表示の代わりに用いている。

【0 1 3 1】

そして、 $F_p^m$ の元 $\alpha$ を基底変換行列によって $F_p^m$ の対応する元 $\beta$ に写像すれば、 $F_p$ 上の $m$ 次既約多項式 $f(x)$ の1つの解を $F_p^m$ 上で求めたこととなる。

【0 1 3 2】

20

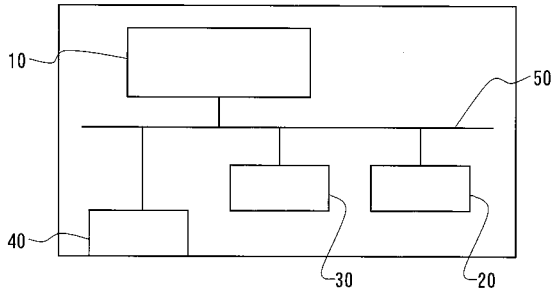
したがって、共役元まで考えれば、 $f(x)$ を $F_p^m$ 上で因数分解できることとなるので、任意の拡大体上で因数分解できることとなる。

【産業上の利用可能性】

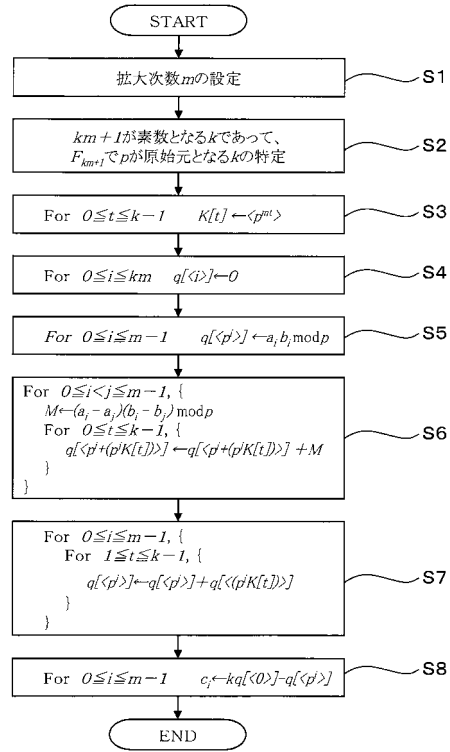
【0 1 3 3】

パーソナルコンピュータや携帯電話、あるいはICチップ付きのクレジットカードのように、他の機器とデータの送受信が行われる機器において、鍵長を任意に変更可能として、要求される安全性と、暗号化または復号化の処理負荷を調整ながら、暗号化データの送受信を可能とする。

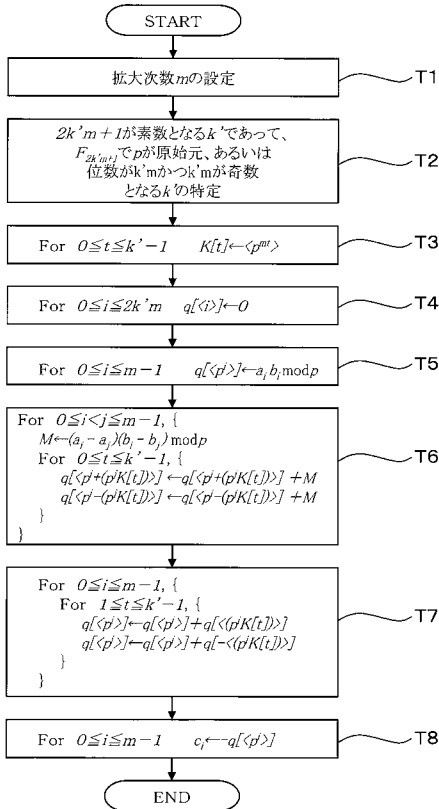
【 図 1 】



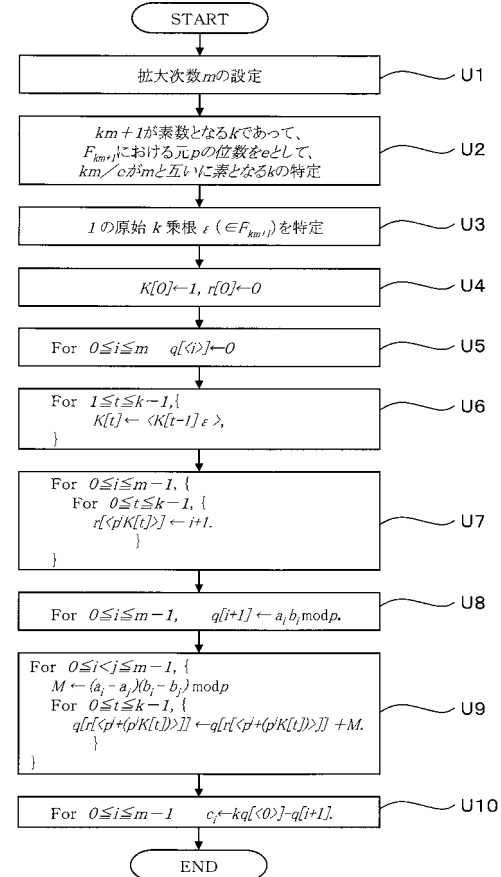
【 図 2 】



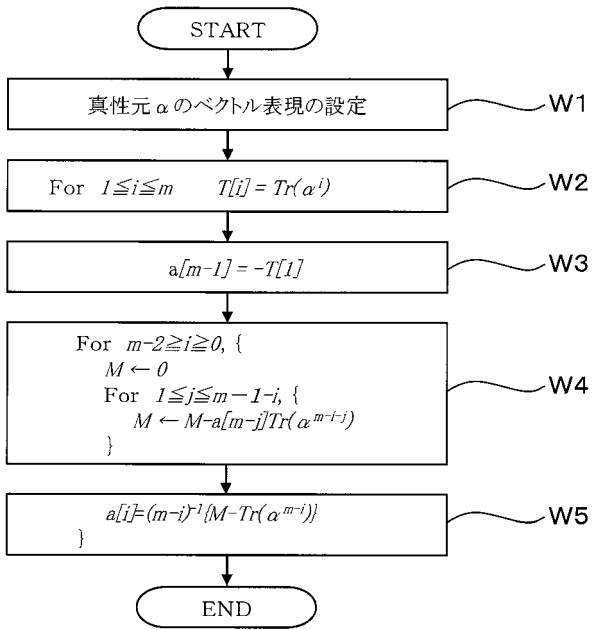
【 図 3 】



【 図 4 】



【 図 5 】



## 【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2007/064474
<b>A. CLASSIFICATION OF SUBJECT MATTER</b> G09C1/00(2006.01) i, G06F7/72(2006.01) i  According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) G09C1/00, G06F7/72		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2007 Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-284111 A (Japan Science and Technology Agency), 13 October, 2005 (13.10.05), Full text (Family: none)	1-11
A	JP 2004-233428 A (NEC Corp.), 19 August, 2004 (19.08.04), Full text (Family: none)	1-11
A	JP 2003-84666 A (Japan Science and Technology Corp.), 19 March, 2003 (19.03.03), Full text (Family: none)	1-11
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family 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 application or patent 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 09 October, 2007 (09.10.07)		Date of mailing of the international search report 16 October, 2007 (16.10.07)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2007/064474

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-304120 A (Japan Science and Technology Corp.), 18 October, 2002 (18.10.02), Full text (Family: none)	1-11



国際調査報告		国際出願番号 PCT/J P 2 0 0 7 / 0 6 4 4 7 4	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G09C1/00(2006.01)i, G06F7/72(2006.01)i			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G09C1/00, G06F7/72			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2007年 日本国実用新案登録公報 1996-2007年 日本国登録実用新案公報 1994-2007年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
A	JP 2005-284111 A (独立行政法人科学技術振興機構) 2005.10.13, 全文 (ファミリーなし)	1-11	
A	JP 2004-233428 A (日本電気株式会社) 2004.08.19, 全文 (ファミリーなし)	1-11	
A	JP 2003-84666 A (科学技術振興事業団) 2003.03.19, 全文 (ファミリーなし)	1-11	
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリ 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献			
国際調査を完了した日 09.10.2007		国際調査報告の発送日 16.10.2007	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 石田 信行	5 S 9 4 6 9
		電話番号 03-3581-1101 内線 3546	

国際調査報告		国際出願番号 PCT/JP2007/064474
C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-304120 A (科学技術振興事業団) 2002.10.18, 全文 (ファミリーなし)	1-11

## フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(出願人による申告)平成17年度、総務省戦略的情報通信研究開発推進制度「公開鍵暗号系での利用を目的とした汎用拡大の構成に関する研究開発」に係る委託研究、産業技術力強化法第19条の適用を受けるもの

(注)この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。