(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5073669号
(P5073669)

(45)発行日　平成24年11月14日(2012.11.14)　(24)登録日　平成24年8月31日(2012.8.31)

(51)Int.Cl.　F I

H04L 9/30	(2006.01)	H04L	9/00	663A
G09C 1/00	(2006.01)	G09C	1/00	620A
		G09C	1/00	650A

請求項の数 14　(全 11 頁)

(21)出願番号　特願2008-538237 (P2008-538237)
(86)(22)出願日　平成18年11月3日 (2006.11.3)
(65)公表番号　特表2009-515206 (P2009-515206A)
(43)公表日　平成21年4月9日 (2009.4.9)
(86)国際出願番号　PCT/CA2006/001805
(87)国際公開番号　WO2007/051305
(87)国際公開日　平成19年5月10日 (2007.5.10)
審査請求日　平成21年10月26日 (2009.10.26)
(31)優先権主張番号　60/732,715
(32)優先日　平成17年11月3日 (2005.11.3)
(33)優先権主張国　米国 (US)

(73)特許権者　397071791
サーティコム　コーポレーション
カナダ国　エル４ダブリュー　Ｏビー５
オンタリオ，ミシソーガ，タホー　ブールバード　４７０１，タホー　エー，　６ティーエイチ　フロア
(74)代理人　100107489
弁理士　大塩　竹志
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100134005
弁理士　澤田　達也
(74)代理人　100151677
弁理士　播磨　里江子

最終頁に続く

(54)【発明の名称】同時スカラー乗算方法

(57)【特許請求の範囲】
【請求項１】
暗号モジュールによって実行される方法であって、前記方法は、
第１のスカラーｋに楕円曲線Ｅ上の第１の点Ｐを乗算する第１の乗算と、第２のスカラーｓに楕円曲線Ｅ上の第２の点Ｑを乗算する第２の乗算とを同時に実行することを含み、前記スカラーｋ、ｓは、異なる数のビットを含み、
前記実行することは、
初期の計算対を生成することであって、前記初期の計算対を生成することは、
前記スカラーｋ、ｓのうち少ない数のビットを含む一方を決定することと、
スカラーｋ、ｓのビット長が等しくなるように前記スカラーの前記一方をゼロでパディングすることにより、ｔビット対（k_i，s_i）を提供することであって、ｔは、前記スカラーのビットの総数を表し、ｉは、前記スカラーの前記一方および前記スカラーの他方において評価されている現在のビットを表す、ことと、
前記スカラーの前記一方における前記パディングと前記スカラーの前記他方の対応するビットとを含むビット対に対してモンゴメリ法を実行することにより、前記初期の計算対を生成することと
によって行われる、ことと、
残りのビット対（k_i，s_i）に対して、前記パディングの後の第１のビット対を開始点として、各ビット対（k_i，s_i）においてそれぞれ示される値に従って前記第１および第２の乗算において少なくとも１回の繰り返し演算を同時に実行することにより、前記

乗算の各ステップにおける数学演算の回数を減らすことによって、前の計算対から（Ｐ＋Ｑ）だけ異なる第１の成分および第２の成分を含む計算対を生成することと
を含む、方法。
【請求項２】
前記スカラーの前記一方における最上位ビットを破棄することと、前記スカラーの前記他方における最上位ビットを破棄することとをさらに含む、請求項１に記載の方法。
【請求項３】
前記計算対は、［ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ］として各ステップにおいて前記第１および第２の乗算を表し、ｍは、前記前の計算対における前記第１の点Ｐの係数を表し、ｎは、前記前の計算対における前記第２の点Ｑの係数を表す、請求項１または請求項２に記載の方法。
【請求項４】
前記ビット対（k_i，s_i）が現在（０，０）に等しいとき、次の計算対は、［２ｍＰ＋２ｎＱ，（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ］である、請求項３に記載の方法。
【請求項５】
前記ビット対（k_i，s_i）が現在（１，１）に等しいとき、次の計算対は、［（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ，（２ｍ＋２）Ｐ＋（２ｎ＋２）Ｑ］である、請求項３に記載の方法。
【請求項６】
前記ビット対（k_i，s_i）が現在（０，１）に等しいとき、次の計算対は、［２ｍＰ＋２ｎＱ＋Ｑ，（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ＋Ｑ］である、請求項３に記載の方法。
【請求項７】
前記ビット対（k_i，s_i）が現在（１，０）に等しいとき、次の計算対は、［２ｍＰ＋２ｎＱ＋Ｐ，（２ｍ＋１）Ｐ＋Ｐ＋（２ｎ＋１）Ｑ］である、請求項３に記載の方法。
【請求項８】
第１のスカラーｋに楕円曲線Ｅ上の第１の点Ｐを乗算する第１の乗算と、第２のスカラーｓに楕円曲線Ｅ上の第２の点Ｑを乗算する第２の乗算とを同時に実行するように構成された暗号モジュールであって、前記スカラーｋ、ｓは、異なる数のビットを含み、
前記暗号モジュールは、
初期の計算対を生成する手段であって、前記初期の計算対を生成することは、
前記スカラーｋ、ｓのうち少ない数のビットを含む一方を決定することと、
スカラーｋ、ｓのビット長が等しくなるように前記スカラーの前記一方をゼロでパディングすることにより、ｔビット対（k_i，s_i）を提供することであって、ｔは、前記スカラーのビットの総数を表し、ｉは、前記スカラーの前記一方および前記スカラーの他方において評価されている現在のビットを表す、ことと、
前記スカラーの前記一方における前記パディングと前記スカラーの前記他方の対応するビットとを含むビット対に対してモンゴメリ法を実行することにより、前記初期の計算対を生成することと
によって行われる、手段と、
残りのビット対（k_i，s_i）に対して、前記パディングの後の第１のビット対を開始点として、各ビット対（k_i，s_i）においてそれぞれ示される値に従って前記第１および第２の乗算において少なくとも１回の繰り返し演算を同時に実行することにより、前記乗算の各ステップにおける数学演算の回数を減らすことによって、前の計算対から（Ｐ＋Ｑ）だけ異なる第１の成分および第２の成分を含む計算対を生成する手段と
を含む、暗号モジュール。
【請求項９】
前記スカラーの前記一方における最上位ビットを破棄することと、前記スカラーの前記他方における最上位ビットを破棄することとを行う手段をさらに含む、請求項８に記載の暗号モジュール。
【請求項１０】

前記計算対は、［ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ］として各ステップにおいて前記第１および第２の乗算を表し、ｍは、前記前の計算対における前記第１の点Ｐの係数を表し、ｎは、前記前の計算対における前記第２の点Ｑの係数を表す、請求項８または請求項９に記載の暗号モジュール。

【請求項１１】

前記ビット対（k_i，s_i）が現在（０，０）に等しいとき、次の計算対は、［２ｍＰ＋２ｎＱ，（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ］である、請求項１０に記載の暗号モジュール。

【請求項１２】

前記ビット対（k_i，s_i）が現在（１，１）に等しいとき、次の計算対は、［（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ，（２ｍ＋２）Ｐ＋（２ｎ＋２）Ｑ］である、請求項１０に記載の暗号モジュール。

【請求項１３】

前記ビット対（k_i，s_i）が現在（０，１）に等しいとき、次の計算対は、［２ｍＰ＋２ｎＱ＋Ｑ，（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ＋Ｑ］である、請求項１０に記載の暗号モジュール。

【請求項１４】

前記ビット対（k_i，s_i）が現在（１，０）に等しいとき、次の計算対は、［２ｍＰ＋２ｎＱ＋Ｐ，（２ｍ＋１）Ｐ＋Ｐ＋（２ｎ＋１）Ｑ］である、請求項１０に記載の暗号モジュール。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、概して暗号法の分野に関するものであり、そのための楕円曲線暗号及びスカラー乗算法における特別な有用性を有する。

【背景技術】

【０００２】

楕円曲線算法で、点乗算（ｐｏｉｎｔ　ｍｕｌｔｉｐｌｉｃａｔｉｏｎ）とは、整数に楕円曲線上の或る点を掛ける演算のことである。この点乗算が楕円曲線暗号スキームの実行時間の大半を占めることは周知である。

【０００３】

値ｋＰを計算するために点乗算を行う１つの方法に、モンゴメリ法があり、ｋは整数、Ｐは楕円曲線Ｅ上の或る点である。モンゴメリ法の１つの実装では、整数値ｋは、基数を２とする一連のバイナリビットで表される。モンゴメリのスカラー乗算は、対（ｍＰ，（ｍ＋１）Ｐ）で始まるシーケンス及びｋのビットを用いてｋＰを計算する。係数ｍは、前の対の第１項における、Ｐの係数を表す任意の整数である。このシーケンスで、各対は、前の対の一方の成分を２倍にし、且つ両成分を加算することによって得られる。ここで、これら演算の順序は、ｋのビット値に依存する。演算のシーケンスは開始対から始まり、最上位ビットを除く、ｋの各ビットごとに新規の対を計算する。全ての対にとって、第２の成分は第１の成分とはＰだけ異なるようになっている。このことは、点倍加及び点加算により効率的な方法を用いることを可能にする。

【０００４】

実際上、演算シーケンスは対（Ｐ，２Ｐ）で開始し、ここに、Ｐは第１項、２Ｐは第２項であり、従ってｍ＝１である。整数ｋの最上位ビットは破棄され、ｋの２番目の上位ビットから最下位ビットへと進み、次の対は以下のように計算される。

【０００５】

各ステップに対し、ｋの現在のビットがゼロ（０）の場合（例えば、２番目のステップに対し、ｋの２番目の上位ビットがゼロの場合）、現在の第１項は前の第１項の２倍とし、現在の第２項は前の第１と第２項の和とする。しかし、ｋの現在のビットが１の場合には、現在の第１項は前の第１と第２項の和とし、現在の第２項は前の第２項の２倍とする

。

【０００６】

例えば、対（ｍＰ，（ｍ＋１）Ｐ）で開始し、ｋの現在のビットが０の場合、次のステップでは、現在の対は（２＊ｍＰ，ｍＰ＋（ｍ＋１）Ｐ）＝（２ｍＰ，（２ｍ＋１）Ｐ）となる。一方、ｋの現在のビットが１の場合には、現在の対は（ｍＰ＋（ｍ＋１）Ｐ，２＊（ｍ＋１）Ｐ）＝（（２ｍ＋１）Ｐ，（２ｍ＋２）Ｐ）となる。これから明らかなように、各ステップは、倍加演算及び加算演算を含む。演算シーケンスは、ｋの最終ビットまで各ビットに対して継続し、その時点（ｋの最後のビットの時点）で、現在の対の第１項（例えば、計算した最後の対の第１項）が、ｋＰに対する所望の値を含むようになる。

【０００７】

モンゴメリ法の一例を、図１に示してある。図１に示す例では、ｋ＝４５＝10110_2である。演算シーケンスは対（Ｐ，２Ｐ）で開始し、ステップｉ＝５～ｉ＝０の間に、ｋの現在のビットに対する新規の対を計算する。

【０００８】

上述した一般的なやり方を説明するために、ステップｉ＝３を参照するに、ここで、ｋの現在のビットは１であり、前の対（すなわちｉ＝４からの対）は（２Ｐ，３Ｐ）である。現在のビットが１なので、図１の表のステップｉ＝３に示すように、現在の第１項は２Ｐ＋３Ｐ＝５Ｐと計算される。現在の第２項は、同様に表に示すように、２＊３Ｐ＝６Ｐと計算される。これらの項の他の計算方法はｍの値に基づき、このステップに対するｍの値は２である（すなわち、ステップｉ＝４におけるＰの係数は２である）。従って、現在の第１項は（２＊２＋１）Ｐ＝５Ｐと計算され、現在の第２項は（２＊２＋２）Ｐ＝６Ｐと計算される。ステップｉ＝０では、ｋ＝４５から予想されるように、値４５Ｐは所望値ｋｐに相当する。

【０００９】

楕円曲線ディジタル署名アルゴリズム（ＥＣＤＳＡ）の検証のような、ある楕円曲線暗号演算では、ｋＰ＋ｓＱを求めるためにスカラー乗算の組み合わせを計算する。ここでＱは、楕円曲線Ｅ上の他の点であり、ｓは他のスカラーである。ｋＰ＋ｓＱを求めるためにモンゴメリ法を用いることができるが、各スカラー乗算は、別々に行うことになり、この場合に得られる２つの値、すなわちｋＰ及びｓＱは、同時乗算(ｓｉｍｕｌｔａｎｅｏｕｓ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ)ｋＰ＋ｓＱを求めるために、互いに加算することになる。従って、ｋＰ＋ｓＱを求めるためには、ｋ及びｓ双方の各ビットに対して、個別に倍加演算と加算演算を必要とする。

【００１０】

スカラー乗算は、楕円曲線暗号スキームの実行時間の大半を占めることになるから、上述したように検証ステップにモンゴメリ法を用いることは、典型的な用途にとっては、非効率的であると見なされる。

【００１１】

従って、本発明の目的は、上述の不利な点の少なくとも１つを取り除くか又は軽減することにある。

【発明の開示】

【発明が解決しようとする課題】

【００１２】

モンゴメリ法での特別な用法である同時点乗算（ｓｉｍｕｌｔａｎｅｏｕｓ ｐｏｉｎｔ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ）の方法を提供する。この方法は、各々の点乗算に対して個別にモンゴメリ法を用いる場合と比較して、倍加演算の回数を減少させ、場合によっては加算演算の回数を減少させる。

【課題を解決するための手段】

【００１３】

本発明の一形態では、第１のスカラーｋに楕円曲線Ｅ上の第１の点Ｐを掛ける第１の乗算と、第２のスカラーｓに楕円曲線Ｅ上の第２の点Ｑを掛ける第２の乗算とを同時に行う

方法を提供する。当該方法は、ｔは前記スカラーのビットの総数を表し、ｉは前記第１及び第２スカラーにおける評価する現在のビットを表すものとして、ｔ個のビット対（k_i，s_i）に対して、前記各ビット対（k_i，s_i）に示す値に従って、前記第１及び第２の乗算にて少なくとも１回の繰り返し演算を同時に行って、前記乗算の各ステップでの数学演算の回数を減らすようにする、同時スカラー乗算方法である。

【００１４】

他の形態では、第１のスカラーｋに楕円曲線Ｅ上の第１の点Ｐを掛ける第１の乗算と、第２のスカラーｓに楕円曲線Ｅ上の第２の点Ｑを掛ける第２の乗算とを同時に行う方法であって、前記第１及び第２のスカラーは異なるビット長であり：各スカラーがｔビットから成るように、前記第１及び第２のスカラーの短い方のスカラーをｖ個のゼロでパディングするステップであって、ｔは最大ビット長のビット総数を表すものとするステップと、前記第１のスカラーｋ及び前記第２のスカラーｓの最上位ビットをそれぞれ破棄するステップと、ｉは前記第１及び第２のスカラーにおける評価する現在のビットを表すものとして、破棄されていないパディングしたゼロを含む、ｖ－１個のビット対（k_i，s_i）に対して、前記第１及び第２のスカラーの長い方のスカラーに対しモンゴメリ法を行うステップと、残りのｔ－ｖ－１個のビット対（k_i，s_i）に対して、前記ビット対（k_i，s_i）に示される値に従って、前記第１及び第２の乗算にて少なくとも１回の繰り返し演算を同時に行って、前記乗算の各ステップでの数学演算の回数を減らすステップと、を含むようにする。

【発明を実施するための最良の形態】

【００１５】

添付の図面を参照して、本発明の実施例を説明する。

【００１６】

図２には、暗号通信システムを１０で総称して示してある。当該システム１０は、通信路１６を介して相互に通信することができる、第１のコレスポンデント１２及び第２のコレスポンデント１４を備えている。通信路１６は（セキュリティ上）安全か、又は安全でないかもしれない。各コレスポンデントは、暗号演算を行うための暗号モジュール１８及び２０を各々備えている。

【００１７】

好ましくは各暗号モジュール１８及び２０は、１以上の整数と、フィールドF_qにわたって規定される楕円曲線Ｅ上の１つ以上の点との点乗算のような、楕円曲線暗号演算を行うことができるようにする。このような暗号演算は、例えば、ＥＣＤＳＡ法及び、このために行う複数のステップを含む。ここに記載する実施例は、特に、組み合わせｋＰ＋ｓＱを計算し、Ｐ及びＱに対して予め計算したテーブルを利用できない場合の、ＥＣＤＳＡの検証に適している。

【００１８】

当然のことながら、ここで記載する実施例は、重複点（ｍｕｌｔｉｐｌｅ　ｐｏｉｎｔ）乗算を含む他の暗号演算にも用いることができ、ここで記載するような、ＥＣＤＳＡの検証のための組み合わせｋＰ＋ｓＱを計算することに限定すべきではない。

【００１９】

本出願人は、モンゴメリ法を用いてｋＰとｓＱを別々に計算する場合に、ｋＰ及びｓＱの計算における幾つかの演算が繰り返され、これは単一演算で実行可能であることを発見した。以下に、倍加演算及び加算演算の総数を減らし、これにより、重複スカラー（ｍｕｌｔｉｐｌｅ　ｓｃａｌａｒ）乗算のための効率的な方法を提供する、同時スカラー乗算法について述べる。

【００２０】

現在の同時スカラー乗算法では、ｋＰ及びｓＱを計算するのに用いる対を組み合わせて、単一の計算対、即ち、（ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ）を生成する。従って、ｍ＝ｎ＝１では、開始対は（Ｐ＋Ｑ，２（Ｐ＋Ｑ））となり、ｋ及びｓの最上位ビットは破棄される。この方法における全ての対にとって、第２成分は第１成分とはＰ＋Ｑだ

け異なるようになっている。このことは、点倍加及び点加算に、より効率的な式を用いることを可能にする。

【００２１】

本実施例では、整数ｋ及びｓを、一連のバイナリビットで表わす。従って、同時スカラー乗算法の各ステップでは、ｋからの１ビットと、ｓからの１ビットとのビット対（k_i，s_i）を参照する。各ステップで２ビットを参照し、且つそのために各ビットがバイナリ表現を有する場合、この例で可能なビット対は、（０，０）、（１，１）、（０，１）、（１，０）である。一般に、各スカラーにはｔビットあり、評価は、ｉ＝ｔ－１からｉ＝０まで進められ、例えば、ここでk_tは最上位ビットであり、k_0は最下位ビットである。

【００２２】

ビットの対が（０，０）、（１，１）である場合には、ｋ及びｓに対して同様な演算を行うのだから、1回の倍加演算をＰ及びＱの双方で同時に行い、前の対の両項を１回加算することができる。従って、Ｐ及びＱの計算には、１回の倍加演算と１回の加算を必要とするだけであるので、ビットの対が（０，０）、（１，１）である場合の、ｋＰ＋ｓＱの本例の同時スカラー乗算は、半分の倍加演算と半分の加算を必要とするだけである。

【００２３】

ビット対が（０，０）の場合、Ｐ及びＱに対する現在の第１項の各々は、前の第１項の倍加演算を必要とし、第２項の各々は、前の第１項と第２項との和となる。従って、対（ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ）で開始すると、ｋ及びｓ双方の現在のビットがゼロ（０）の場合、次の対は、（２＊（ｍＰ＋ｎＱ），ｍＰ＋ｎＱ＋（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ）となり、これは簡約すると次のようになる。

ケース１（０，０）：（２ｍＰ＋２ｎＱ，（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ）；

ここでｍ及びｎは、前のステップにおけるＰ及びＱの各々の係数である。

【００２４】

ビット対が（１，１）の場合、Ｐ及びＱに対する現在の第１項の各々は、前の第１項と第２項との和となり、第２項の各々は、前の第２項を２倍したものを必要とする。従って、対（ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ）で開始すると、ｋ及びｓ双方の現在のビットが（１）の場合、次の対は、（ｍＰ＋ｎＱ＋（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ，２＊（（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ））となり、これは簡約すると、次のようになる。

ケース２（１，１）：（（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ，（２ｍ＋２）Ｐ＋（２ｎ＋２）Ｑ）；

ここでｍ及びｎは、前のステップにおけるＰ及びＱの各々の係数である。

【００２５】

従って、ｋとｓのビットが同じ場合には、ｋＰ＋ｓＱを計算するシーケンスにおいて現在のステップを計算するのに半分の演算で済むことになり、これにより、重複点スカラー乗算の計算効率が増大する。

【００２６】

ビット対が（０，１）及び（１，０）の場合、ｋＰ及びｓＱには異なる演算を必要とするが、特に、繰り返される倍加演算では、所定の繰り返しを避けることができる。ビット対が（０，１）及び（１，０）の場合に、ｋＰ＋ｓＱの本例の同時スカラー乗算は半分の倍加演算を必要とするだけであり、従って、総合演算のうち４分の３の演算回数で済む。

【００２７】

ビット対が（０，１）の場合、Ｐ及びＱに対する現在の第１項は、倍加及び加算演算をそれぞれ必要とし、Ｐ及びＱに対する現在の第２項は、その逆を必要とする。Ｐ及びＱの双方を同時に適合させるために、本出願人は、現在の第１項は、前の第１項を２倍し、Ｑを加えることによって計算することができ、現在の第２項は、（Ｐ＋Ｑ）を現在の第１項に加えることによって計算することができ、これにより、１回の倍加と２回の加算を必要とするだけで済むことを発見した。従って、対（ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ）で開始すると、（ｋの現在のビットがゼロ（０）で、ｓの現在のビットが（１）の場

合の）次の対は、（２＊（ｍＰ＋ｎＱ）＋Ｑ，２＊（ｍＰ＋ｎＱ）＋Ｑ＋（Ｐ＋Ｑ））となり、これは簡約すると、次のようになる。
ケース３（０，１）：（２ｍＰ＋２ｎＱ＋Ｑ，（２ｍ＋１）Ｐ＋（２ｎ＋１）Ｑ＋Ｑ）；
ここでｍ及びｎは、前のステップにおけるＰ及びＱの各々の係数である。

【００２８】

ビット対が（１，０）の場合、Ｐ及びＱに対する現在の第１項は、加算及び倍加演算をそれぞれ必要とし、Ｐ及びＱに対する現在の第２項には、その逆を必要とする。ＰとＱの双方を同時に適合させるために、本出願人は、現在の第１項は、前の第１項を２倍し、Ｐを加えることによって計算することができ、現在の第２項は、（Ｐ＋Ｑ）を現在の第１項に加えることによって計算することができ、これにより、１回の倍加と２回の加算を必要とするだけで済むことを発見した。従って、対（ｍＰ＋ｎＱ，（ｍ＋１）Ｐ＋（ｎ＋１）Ｑ）で開始すると、（ｋの現在のビットが（１）で、ｓの現在のビットがゼロ（０）の場合の）次の対は、（２＊（ｍＰ＋ｎＱ）＋Ｐ，２＊（ｍＰ＋ｎＱ）＋Ｐ＋（Ｐ＋Ｑ））となり、これは簡約すると、次のようになる。
ケース４（１，０）：（２ｍＰ＋２ｎＱ＋Ｐ，（２ｍ＋１）Ｐ＋Ｐ＋（２ｎ＋１）Ｑ）；
ここでｍ及びｎは、前のステップにおけるＰ及びＱの各々の係数である。

【００２９】

従って、ｋ及びｓのビットが異なる場合に、ｋＰ＋ｓＱを計算するシーケンスにおいて現在のステップを計算するのに、４分の３の演算で済むことになる。これにより、重複点スカラー乗算の計算効率が増大する。

【００３０】

演算シーケンスは、（上記のどのケースを必要とするかを評価する）各ビット対に対して、ｋ及びｓの最下位ビットまで続き、その時点（ｋ及びｓの最小ビットになった時点）で、現在の対（例えば最後に計算した対）が、その対の第１項として所望値ｋＰ＋ｓＱを含むようになる。

【００３１】

上述した実施例の一例を、図３に示してある。図３に示した例では、ｋ＝４５＝１０１１０１$_2$、ｓ＝５４＝１１０１１０$_2$とし、ｋ及びｓのビット長は同じで、ｔ＝６としてある。シーケンスは、対（Ｐ＋Ｑ，２Ｐ＋２Ｑ）で開始し、ステップｉ＝５からステップｉ＝０までの間に、現在のビットに対する新たな対を以下のように計算する。

【００３２】

ｋの最上位ビット及びｓの最上位ビットは破棄し、最初の計算はステップｉ＝４で開始する。このステップでは、ｋの現在のビットはゼロ（０）であり、ｓの現在のビットは（１）であり、前の対（すなわち開始時の対）は（Ｐ＋Ｑ，２Ｐ＋２Ｑ）である。現在のビット対は（０，１）なので、現在の第１項は、前の第１項を２倍して、Ｑを加えることにより計算され、すなわち、図３の表のステップｉ＝４に示すように、２＊Ｐ＋２＊Ｑ＋Ｑ＝２Ｐ＋３Ｑとなる。現在の第２項は、現在の第１項に（Ｐ＋Ｑ）を加えることにより計算され、すなわち、同じく表に示すように、２Ｐ＋３Ｑ＋（Ｐ＋Ｑ）＝３Ｐ＋４Ｑとなる。それぞれの項を計算するための他の方法は、ｍ及びｎの値に基づき、このステップではそれぞれ１に等しい（すなわち、ステップｉ＝５におけるＰ及びＱの係数）。従って、現在の第１項は２＊１Ｐ＋２＊１Ｑ＋Ｑ＝２Ｐ＋３Ｑと計算され、現在の第２項は、上記で計算したように、（２＊１＋１）Ｐ＋（２＊１＋１）Ｑ＋Ｑ＝３Ｐ＋４Ｑと計算される。

【００３３】

ステップｉ＝３では、ｋの現在のビットは（１）、ｓの現在のビットは（０）、前の対は（２Ｐ＋３Ｑ，３Ｐ＋４Ｑ）である。現在のビット対は（１，０）なので、現在の第１項は、前の第１項を２倍してＰを加えることにより計算され、すなわち、図３の表のステップｉ＝３に示すように、２＊２Ｐ＋２＊３Ｑ＋Ｐ＝５Ｐ＋６Ｑとなる。現在の第２項は、現在の第１項に（Ｐ＋Ｑ）を加えることにより計算され、すなわち、同じく表に示すよ

うに、５Ｐ＋６Ｑ＋（Ｐ＋Ｑ）＝６Ｐ＋７Ｑとなる。当然のことながら、当該対は、上述したようにｍ及びｎの値に基づいて計算することもできる。

【００３４】

ステップｉ＝２では、ｋの現在のビットは（１）、ｓの現在のビットは（１）、前の対は（５Ｐ＋６Ｑ，６Ｐ＋７Ｑ）である。現在のビット対は（１，１）なので、現在の第１項は、前の両項の和として計算され、すなわち、図３の表のステップｉ＝２に示すように、５Ｐ＋６Ｐ＋６Ｑ＋７Ｑ＝１１Ｐ＋１３Ｑとなる。現在の第２項は、前の第２項を２倍することにより計算され、すなわち、同じく表に示すように、２＊６Ｐ＋２＊７Ｑ＝１２Ｐ＋１４Ｑとなる。当然のことながら、当該対は、上述したようにｍ及びｎの値に基づいて計算することもできる。

【００３５】

ステップｉ＝１では、ｋの現在のビットは（０）、ｓの現在のビットは（１）、前の対は（１１Ｐ＋１３Ｑ，１２Ｐ＋１４Ｑ）である。現在のビット対は（０，１）なので、現在の第１項は、前の第１項を２倍してＱを加えることにより計算され、すなわち、図３の表のステップｉ＝１に示すように、２＊１１Ｐ＋２＊１３Ｑ＋Ｑ＝２２Ｐ＋２７Ｑとなる。現在の第２項は、現在の第１項に（Ｐ＋Ｑ）を加えることにより計算され、すなわち、同じく表に示すように、２２Ｐ＋２７Ｑ＋（Ｐ＋Ｑ）＝２３Ｐ＋２８Ｑとなる。当然のことながら、当該対は、上述したようにｍ及びｎの値に基づいて計算することもできる。

【００３６】

最後に、ステップｉ＝０では、ｋの現在のビットは（１）、ｓの現在のビットは（０）、前の対は（２２Ｐ＋２７Ｑ，２３Ｐ＋２８Ｑ）である。現在のビット対は（１，０）なので、現在の第１項は、前の第１項を２倍してＰを加えることにより計算され、すなわち、図３の表のステップｉ＝０に示すように、２＊２２Ｐ＋２＊２７Ｑ＋Ｐ＝４５Ｐ＋５４Ｑとなる。現在の第２項は、現在の第１項に（Ｐ＋Ｑ）を加えることにより計算され、すなわち、同じく表に示すように、４５Ｐ＋５４Ｑ＋（Ｐ＋Ｑ）＝４６Ｐ＋５５Ｑとなる。当然のことながら、当該対は、上述したようにｍ及びｎの値に基づいて計算することもできる。

【００３７】

値４５Ｐ＋５４Ｑ（すなわち、最後の対の第１項）は、ｋ＝４５及びｓ＝５４であることから予測される、所望の組み合わせｋＰ＋ｓＱに相当する。

【００３８】

図４に示す他の実施例では、ｋ及びｓのビット長が異なり、ｋ＝５＝１０１$_2$、ｓ＝１０９＝１１０１１０１$_2$とする。この場合には、ビット長が等しくなるように、最初にｋをｖ個の０でパディングする。表に示すように、ステップｉ＝６からｉ＝３に対して（すなわち、パディングした０及びｋの第１項に対して）、モンゴメリ法をＱのみに対して（すなわち、長いビット長を有し、従って０を埋め込んでいないスカラーに対して）実施する。

【００３９】

従って、演算シーケンスは、ステップｉ＝６にて対（Ｑ，２Ｑ）で開始する。最上位ビットは破棄するので、最初の計算はステップｉ＝５から開始する。ステップｉ＝５でのｋのビットはゼロでパディングしてあるので、ｓのビットだけに着目する。このステップでは、ｓのビットは（１）であり、前の対（すなわち第１の対）は（Ｑ，２Ｑ）である。ｓのビットは（１）なので、現在の第１項は、前の両項の和として計算され、すなわち、図４の表のステップｉ＝５に示すように、Ｑ＋２Ｑ＝３Ｑとなる。現在の第２項は、前の第２項を２倍することにより計算され、すなわち、同じく表に示すように、２（２Ｑ）＝４Ｑとなる。当然のことながら、当該対は、ｎの値に基づいて計算することもできる。

【００４０】

ステップｉ＝４では、ｋのビットは同じくゼロでパディングしてあるので、ｓのビットだけに着目する。このステップで、ｓのビットはゼロ（０）、前の対は（３Ｑ，４Ｑ）である。ｓのビットがゼロ（０）なので、現在の第１項は、前の第１項を２倍することによ

り計算され、すなわち、図４の表のステップｉ＝４に示すように、２＊３Ｑ＝６Ｑとなる。現在の第２項は、前の両項の和として計算され、すなわち、同じく表に示すように、３Ｑ＋４Ｑ＝７Ｑとなる。当然のことながら、当該対は、ｎの値に基づいて計算することもできる。

【００４１】

ステップｉ＝３では、ｋのビットはこのシーケンスに対する最後にパディングしたビットであり、従って、ｓのビットだけに着目する。このステップで、ｓのビットは（１）、前の対は（６Ｑ，７Ｑ）である。ｓのビットが（１）なので、現在の第１項は、前の両項の和として計算され、すなわち、図４の表のステップｉ＝３に示すように、６Ｑ＋７Ｑ＝１３Ｑとなる。現在の第２項は、前の第２項を２倍することにより計算され、すなわち、同じく表に示すように、２（７Ｑ）＝１４Ｑとなる。当然のことながら、当該対は、ｎの値に基づいて計算することもできる。

【００４２】

ステップｉ＝２では、ｋのビットは、もはやパディングしたゼロではなく、実際の値である。従って、この対が、同時乗算における第１の対であり、ｋの第１ビットを破棄し、対（Ｐ，２Ｐ）を現在のＱ値に加える。現在のＱの値は、現在のｓの値（これは（１）である）及び、前の対（これは（１３Ｑ，１４Ｑ）である）に着目することにより計算される。ｓのビットが（１）なので、現在の第１項のＱの部分は、前の両項の和として計算され、すなわち、図４の表のステップｉ＝２に示すように、１３Ｑ＋１４Ｑ＝２７Ｑとなる。現在の第２項のＱの部分は、前の第２項を２倍することにより計算され、すなわち、同じく表に示すように、２（１４Ｑ）＝２８Ｑとなる。当然のことながら、当該対は、ｎの値に基づいて計算することもできる。それから、完全な対は、現在のＱの値に（Ｐ，２Ｐ）を加えることにより得られ、表に示すように、（Ｐ＋２７Ｑ，２Ｐ＋２８Ｑ）となる。

【００４３】

次のステップ（すなわち、同時乗算部分の第２ステップ）は、ｉ＝１で現在のビット対（０，０）を利用し、前の対は（Ｐ＋２７Ｑ，２Ｐ＋２８Ｑ）である。ビット対が（０，０）なので、現在の第１項は、前の第１項を２倍することにより計算され、すなわち、図４の表のステップｉ＝１に示すように、２＊Ｐ＋２＊２７Ｑ＝２Ｐ＋５４Ｑとなる。現在の第２項は、前の両項の和として計算され、すなわち、同じく表に示すように、Ｐ＋２７Ｑ＋２Ｐ＋２８Ｑ＝３Ｐ＋５５Ｐとなる。当然のことながら、当該対は、上述したようにｍ及びｎの値に基づいて計算することもできる。

【００４４】

最後に、ステップｉ＝０では、現在のビット対は（１，１）で、前の対は（２Ｐ＋５４Ｑ，３Ｐ＋５５Ｑ）である。ビット対が（１，１）なので、現在の第１項は、前の両項の和として計算され、すなわち、図４の表のステップｉ＝０に示すように、２Ｐ＋５４Ｑ＋３Ｐ＋５５Ｑ＝５Ｐ＋１０９Ｑとなる。現在の第２項は、前の第２項を２倍することにより計算され、すなわち、同じく表に示すように、２＊３Ｐ＋２＊５５Ｑ＝６Ｐ＋１１０Ｑとなる。当然のことながら、当該対は、上述したようにｍ及びｎの値に基づいて計算することもできる。

【００４５】

値５Ｐ＋１０９Ｑ（すなわち、最後の対の第１項）は、ｋ＝５及びｓ＝１０９であることから予測される、所望の組み合わせｋＰ＋ｓＱに相当する。従って、本例の同時点乗算法は、異なるビット長の整数に対しても、容易に実装することができる。

【００４６】

ある特定の実施例を参照しながら本発明を説明したが、添付した特許請求の範囲によって規定されるような本発明の精神及び範囲を逸脱することなく、幾多の変更を加えうることは当業者に明らかである。

【図面の簡単な説明】

【００４７】

【図１】スカラー乗算のためのモンゴメリ方法の実装を示す表である。

【図２】暗号通信システムを示す図である。
【図３】同時スカラー乗算法の実施例を示す表である。
【図４】図３に示した同時スカラー乗算法の他の実施例を示す表である。

【図１】

$k = 101101_2 = (k_5k_4k_3k_2k_1k_0)_2 = 45$

ステップ	現在の対	ビット: k_i
i = 5	(P, 2P)	1
4	(2P, 3P)	0
3	(5P, 6P)	1
2	(11P, 12P)	1
1	(22P, 23P)	0
0	(45P, 46P)	1

従来技術(モンゴメリ法)

Figure 1

【図２】

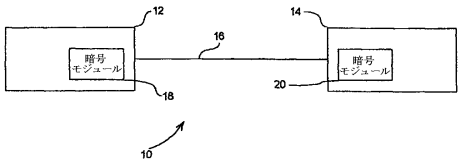

Figure 2

【図３】

シナリオ1:kとsが同じビット長

$k = 101101_2 = (k_5k_4k_3k_2k_1k_0)_2 = 45$
$s = 110110_2 = (s_5s_4s_3s_2s_1s_0)_2 = 54$

ステップ	現在の対	ビット対: k_is_i
i = 5	(P+Q, 2P+2Q)	11
4	(2P+3Q, 3P+4Q)	01
3	(5P+6Q, 6P+7Q)	10
2	(11P+13Q, 12P+14Q)	11
1	(22P+27Q, 23P+28Q)	01
0	(45P+54Q, 46P+55Q)	10

Figure 3

【図４】

シナリオ2:kとsが異なるビット長

$k = 0000101_2 = (k_6k_5k_4k_3k_2k_1k_0)_2 = 5$
$s = 1101101_2 = (s_6s_5s_4s_3s_2s_1s_0)_2 = 109$

ステップ	現在の対	ビット対: k_is_i
i = 6	(Q, 2Q)	01
5	(3Q, 4Q)	01
4	(6Q, 7Q)	00
3	(13Q, 14Q)	01
2	(P+27Q, 2P+28Q)	11
1	(2P+54Q, 3P+55Q)	00
0	(5P+109Q, 6P+110Q)	11

Figure 4

フロントページの続き

(72)発明者 エイドリアン アンティパ
カナダ国 オンタリオ州 エル６ピー ０イー３ ブランプトン ファリーナ ドライヴ １２
(72)発明者 ユーリ ポーレフ
カナダ国 オンタリオ州 エヌ２ティー ２ワイ２ ウォータールー フライブルグ ドライヴ ６３７

審査官 中里 裕正

(56)参考文献 国際公開第００／０２５２０４（WO，Ａ１）
特開２００２－３２３８５２（ＪＰ，Ａ）
特開２００３－１３１５６８（ＪＰ，Ａ）
特開２００３－２８８０１３（ＪＰ，Ａ）
特開２００３－２８８０１４（ＪＰ，Ａ）
特開２００４－０５３８１４（ＪＰ，Ａ）
秋下徹，Ｍｏｎｔｇｏｍｅｒｙ型楕円曲線における高速なスカラー倍同時計算法，情報処理学会研究報告，日本，社団法人情報処理学会 Information Processing Society of Japan，２００１年 ７月２５日，第2001巻 第75号，p.97-103
Toru Akishita, Fast Simultaneous Scalar Multiplication on Elliptic Curve with Montgomery Form, Lecture Notes in Computer Science, ２００１年, Vol.2259, p.255-267

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/30
G09C 1/00
JSTPlus/JMEDPlus/JST7580(JDreamII)