(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3833175号
(P3833175)
(45)発行日　平成18年10月11日(2006.10.11)　(24)登録日　平成18年7月28日(2006.7.28)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 620A
G09C 1/00 650A

請求項の数 6　(全 8 頁)

(21)出願番号　特願2002-509226(P2002-509226)
(86)(22)出願日　平成13年6月21日(2001.6.21)
(65)公表番号　特表2004-502984(P2004-502984A)
(43)公表日　平成16年1月29日(2004.1.29)
(86)国際出願番号　PCT/FR2001/001948
(87)国際公開番号　WO2002/005483
(87)国際公開日　平成14年1月17日(2002.1.17)
審査請求日　平成15年2月24日(2003.2.24)
(31)優先権主張番号　00 08994
(32)優先日　平成12年7月10日(2000.7.10)
(33)優先権主張国　フランス(FR)

(73)特許権者　397062397
ジェムプリュス
ＧＥＭＰＬＵＳ
フランス共和国、エフー１３８８１　ジェムノ　セデックス，パルク　ダクティヴィテ　ドゥ　ジェムノ，アヴニュ　デュ　ピック　ドゥ　ベルターニュ
(74)代理人　100086368
弁理士　萩原　誠
(72)発明者　マルク　ジョワ
フランス　サン　ザカリー　８３６４０　ルー　ヴォルテール　１９
(72)発明者　パスカル　パイエ
フランス　パリ　７５０２０　クール　ドヴァンセンヌ　３７

最終頁に続く

(54)【発明の名称】一定の区間内に含まれる素数から電子キーを生成する方法とその装置

(57)【特許請求の範囲】

【請求項１】

処理用メインユニットと算術プロセッサとを備える携帯型電子装置によって、一定の正の整数の区間［w_m，w_M］内に含まれる素数ｑから電子キーを生成する方法であって、

前記素数ｑは以下の演算を実施する前記携帯型電子装置によって得られ、

前記演算は前記処理用メインユニットと算術プロセッサとによって実施され、

ａ）ε_mがw_m／ηの大きな概数で、ε_Mが（$w_M - w_m$）／ηの小さな概数であるような、２つの正の整数ε_m及びε_Mが存在するために、ｋを最大値とし、ηを最初のｋ個の素数の積とする、正の整数ηを取得する。

$\Pi = \varepsilon_M \cdot \eta$　及び　$\rho = \varepsilon_m \cdot \eta$　を計算する。

ｃをΠと素数関係にあるｃとして、モジュロ整数Πの乗法群Z^*_Πに属する２つの正の整数ａ及びｃを生成する。

ｂ）ｑ＝ｃ＋ρを計算する。

ｑの一次性をテストする。

ｃ）電子キーの生成のために計算されたｑを用いて、一次性を検証する。

ｄ）そうでない場合には、ａ．ｃ　ｍｏｄΠ　を計算することで、ｃを更新し、ｑの一次性が検証されるまで、前記(ｂ)(ｃ)(ｄ)の演算を繰り返す。

ことを特徴とする方法。

【請求項２】

請求項１に記載の方法において、

ａ＝２ 及び Π＝(ε$_M$－１)・η である、ことを特徴とする方法。
【請求項３】
請求項１に記載の方法において、
ａ＝２^{16}＋１である、ことを特徴とする方法。
【請求項４】
請求項１から３のいずれか一項に記載の方法において、
この方法は、ＲＳＡ、El Gamal、Schnorr、またはFiat Shamirのいずれかによる暗号キー生成方法に適用される、ことを特徴とする方法。
【請求項５】
処理用メインユニットと算術プロセッサと関連プログラムメモリと他のメモリとを備え、モジュラ計算を行うことができる携帯型の電子装置であって、
一定の正の整数の区間［W_m，W_M］内に含まれる素数ｑの一次性の検証プログラムを有し、
前記処理用メインユニットと算術プロセッサとによって以下の演算を行う手段を備え、
ａ）ε$_m$ がw_m／ηの大きな概数で、ε$_M$ が（w_M－w_m）／ηの小さな概数であるような、２つの正の素数ε$_m$ 及びε$_M$ が存在するために、ｋを最大値とし、ηを最初のｋ個の素数の積とする、正の整数ηを取得する。
Π＝ε$_M$・η 及び ρ＝ε$_m$・η を計算する。
ｃをΠと素の関係として、モジュロ整数Πの乗法群Z^*_Πに属する２つの正の整数(ａ及びｃ)を生成する。
ｂ） ｑ＝ｃ＋ρを計算する。
ｑの一次性をテストする。
ｃ）電子キーの生成のために計算されたｑを用いて一次性を検証し、一次性が検証された場合には、ｑを前記メモリーに記憶する。
ｄ）そうでない場合には、ａ.ｃ ｍｏｄΠ を計算することで、ｃを更新し、ｑの一次性が検証されるまで、前記(ｂ)(ｃ)(ｄ)の演算を繰り返す。
ことを特徴とする装置。
【請求項６】
請求項５に記載の装置において、
この装置はマイクロプロセッサ付チップカードによって構成される、ことを特徴とする装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、一定の正の整数の区間［w_m、w_M］ に含まれる素数ｑから電子キーを生成する方法に関するものである。本発明はまた、この方法を実施する装置に関するものである。
本発明は、とりわけ、情報の暗号化及び／または２つのエンティティ間の認証及び／またはメッセージの電子シグネーチャのために使用される公開キーによる暗号プロトコルに適用される。
本発明は、特に、ＲＳＡ（Rivest Sahmir & Adelman）、El Gamal、SchnorrまたはFiat Shamirプロトコルのような公開キー(鍵)による暗号解読技術に適用される。
【０００２】
【従来の技術】
このような適用の場合には、一つまたは複数のプロトコルのキーを形成するためには、大きな素数（たとえば５１２ビット以上とすることができる）の生成に頼っている。
素数の生成の「素朴な」第一の方法は、以下からなる。
－奇数から候補を選ぶ、
－その一次性をテストする、
－一次性が検証された場合には、その数が記憶され、そうでない場合には、その候補を２

だけ増分することによって修正し、その新しい候補でテストを繰り返し、候補の一次性が検証されるまで以下同様に続ける。

【０００３】

この方法はとても時間がかかる。他の方法は、素数Πをともなう素数の中から一次性のテストの候補を選択するというものがある。２つの数は、その最大公約数（ｐｇｃｄ）が１である場合、また1である場合にのみ、互いに素であることまたは共素数であることを思い起こされたい。

【０００４】

この方法は以下からなる：

－ｋ個の最初の素数（多くの場合ｋ＝４）の積である数 Π＝２，３，５，７，・・・を対象として、Πをともなう素数ｐのような数ｐを選択する。

－ｐの一次性をテストする。

－ｐの一次性が検証されたら、この数を記憶する、そうでなければΠだけ増分させながらｐを修正する。この新しい候補ｐはまたΠをともなう素数である。実際に、以下が思い起こされる。

ｐｇｃｄ（ｐ＋Π，Π）＝ｐｇｃｄ（ｐ，Π）＝１

－この新しい候補でテストを繰り返し、素数である候補が見つかるまで以下同様に続ける。

この方法はより効果的である。

【０００５】

【発明が解決しようとする課題】

しかしながら、一般に、一定の区間内で素数を生成することが望ましい。というのも、たとえばＲＳＡ公開キーによる暗号プロトコルの場合には、２つの素数ｐ及びｑの１０２４ビットの積、すなわち $2^{511}\cdot\sqrt{2}<p,q<2^{512}$ が対象となる。離散ロガリズムに基づく他のプロトコルによれば、1024ビットの素数、すなわち $2^{1023}<p<=2^{1024}$ を直接的に得ようとする。これらのプロトコルは、512ビット、さらには1024ビット、またはそれ以上の、通常の大きな規模の数については、性能があまり良くないし、マイクロプロセッサ付カード型の携帯装置でプログラミングするのは難しい。なぜなら複雑だからである。

【０００６】

【課題を解決するための手段】

本発明は、区間を［w_m、w_M］として、すべてに対していったんΠを決定し、候補の修正を提案し、その結果、新しい候補が、妥当な限界値内で、すなわち一次性のテスト数を限定しながら、これら新しい候補の計算時間を保ちながらも、当初に決定した区間内でΠと素の関係になるように保証することを目的とする。

Πの選択は図１に示されているが、ここには区間［w_m、w_M］内に含まれる整数の集合Ｉが示され、Πと素の関係にあるこの区間の整数の集合ＩΠが含まれ、この区間の素数の集合ＩＰが含まれる。その目的は、Πをともなう素整数の中間集合ＩΠ、すなわち候補の集合が、この区間の素数の小集合ＩＰにできるだけ近くなるように、Πを決定することにある。

【０００７】

本発明は、処理用メインユニットと算術プロセッサとを備える携帯型電子装置によって、一定の正の整数の区間［w_m，w_M］内に含まれる素数ｑから電子キーを生成する方法であって、

前記素数ｑは以下の演算を実施する前記携帯型電子装置によって得られ、

前記演算は前記処理用メインユニットと算術プロセッサとによって実施され、

主に、素数ｑが以下の演算を行うことによって得られることを特徴とする方法を対象とする。

ａ）ε_mがw_m／ηの大きな概数(higher roundoff)で、ε_Mが（w_M-w_m）／ηの小さな概数(lower roundoff)であるような、２つの正の整数ε_m及びε_Mが存在するため

に、ｋを最大値とし、ηを最初のｋ個の素数の積とする、正の整数ηを選択する。
Π＝ε_M・η 及び ρ＝ε_m・η の計算。
ｃをΠと素の関係とすると、モジュロ整数Πの乗法群Z^*_Πに属する正の２つの整数ａ及びｃの生成。
ｂ）ｑ＝ｃ＋ρ の計算。
ｑの一次性のテスト
ｃ）電子キーの生成のために計算されたｑを用いて一次性を検証し、一次性が検証された場合には、ｑをメモリーに記憶する。
ｄ）そうでない場合には：
ａ．ｃ ｍｏｄ Π を計算することでｃを修正(更新)する。
ｑの一次性が検証されるまで、前記の演算をｂ）から(ｃ）（ｄ)と繰り返す。

【０００８】
本発明の特徴によれば、ａ＝２ 及び Π＝（ε_M－１）・η である。
他の特徴によればａ＝2^{16}＋１ である。
本発明は、ＲＳＡ、El Gamal、SchnorrまたはFiat Shamir暗号キーの生成方法に実施されて適用することができ、暗号解読法として利用できる。

【０００９】
本発明はまた、処理用メインユニットと算術プロセッサと関連プログラムメモリと他のメモリとを備え、モジュラ計算を行うことができる、携帯電子装置であって、
一定の正の整数の区間［W_m，W_M］内に含まれる素数ｑの一次性の検証プログラムを有し、
前記処理用メインユニットと算術プロセッサとによって以下の演算を行う手段を備えることを特徴とする装置を対象とする。
ａ）ε_mがw_m／ηの大きな概数で、ε_Mが（w_M－w_m）／ηの小さな概数であるような、２つの正の素数ε_m及びε_Mが存在するために、ｋを最大値とし、ηを最初のｋ個の素数の積とする、正の整数ηの選択(取得)。
Π＝ε_M・η 及び ρ＝ε_m・ηの計算。
ｃをΠと素の関係として、モジュロ整数Πの乗法群Z^*_Πに属する２つの正の整数ａ及びｃの生成。
ｂ）ｑ＝ｃ＋ρの計算。
ｑの一次性のテスト。
ｃ）電子キーの生成のために計算されたｑを用いて一次性を検証し、一次性が検証された場合には、算術プロセッサがｑをメモリーに記憶する。
ｄ）そうでない場合には：
ａ.ｃ ｍｏｄ Π を計算することでｃを修正(更新)し、ｑの一次性が検証されるまで、前記の演算をｂ）からｃ）ｄ）と繰り返す。
そして、より有利な形態としては、携帯電子装置は、マイクロプロセッサ付チップカードによって構成されるとよい。

【００１０】
【発明の実施の形態】
添付の図面１～３を参照して、以下に限定的でない例として説明することで、本発明の他の特徴及び利点が明らかになるだろう。
図１は、区間［w_m、w_M］内に含まれる整数の集合Ｉと、互いに素のｋの区間の整数の集合ＩΠと、さらにこの区間の素数の集合ＩＰを示す図である。
図２は、本発明による方法のフローチャートである。
図３は、本発明による方法を実施するためのチップカードのような携帯電子装置の原理図である。

【００１１】
本発明の目的は、まず第一に、図１に示されているΠをともなう素数の集合ＩΠが、区間の素数の小集合ＩＰにできるだけ近くなるように、Πを決定することにある。

本発明によれば、図２に示されている方法は、以下の方法で初期化される（第１段階）。
$q \in [w_m, w_M]$ のような素数ｑを生成するために、
ε_m は w_m / η の大きな概数で、$\square w_m / \eta \square$ と記され、ε_M は $(w_M - w_m) / \eta$ の小さな概数で、$\square (w_M - w_m) / \eta \square$ と記されるような２つの正の整数 ε_m 及び ε_M が存在するために、ｋ’を最大値として、２つの正の整数Πと同じ形態の数ηを選択する（ηはｋ’個の最初の素数の積である）。

【００１２】

こうして、$\Pi = \varepsilon_M \cdot \eta$ とすることで Π が得られ、さらに $\rho = \varepsilon_m \cdot \eta$ となる。
Πは、$w_M - w_m$ の近似値だが $w_M - w_m$ より小さく、ρは w_m の近似値だが w_m より大きい。
ここで、新しい候補が常にＩΠに属するように、候補の修正を決定しなければならない。
モジュロ整数Πの環を Z_Π とし、Z_Π の乗法群を Z^*_Π とする。ここで、集合（$\rho + Z^*_\Pi$）は、ＩΠ内に含まれ、ＩΠとほぼ等しくなり、すなわち候補の集合とほぼ等しくなる点が留意される。

【００１３】

こうして、この乗法群 Z^*_Π に属する２つの正の整数ａ及びｃが生成され、この場合、ｃはΠと素の関係の素数であり（すなわちｐｇｃｄ（ｃ，Π）＝１）、候補ｑ＝ｃ＋ρと見なされる（第１段階）。ｃを生成するためには、関連文献に記載されているような共素数の生成アルゴリズムが使用される。
ρは w_m の近似値で、ｃ＜Πであることから、自動的に $w_m < q < w_M$ であることが検証される。
さらに、ｐｇｃｄ（ｑ，Π）＝ｐｇｃｄ（ｃ＋ρ，Π）＝ｐｇｃｄ（ｃ，Π）＝１ である。このようにして、ｑは実際にＩΠに属することが検証される。

【００１４】

この初期化段階が終わると、候補ｑの一次性がテストされる（第２段階）。それが検証されるとｑが記憶される。そうでない場合には、ａ．ｃ ｍｏｄ Π を計算することよってｃを修正し、新しい候補ｑ＝ｃ＋ρを計算する（第３段階）。
新しい候補は、集合ＩΠに属する。とういのも、乗法群の特性によって、ａ及びｃは Z^*_Π に属し、積ａ.ｃはまたこの群 Z^*_Π ならびにａ.ｃ ｍｏｄ Π に属するからである。

【００１５】

公開キーによる暗号プロトコルは、多くの場合、マイクロプロセッサ付チップカード上で使用される。たとえばＲＳＡプロトコルにおいては、キー(鍵)は、プロトコル実行中にマイクロプロセッサ付カードによってアトランダムに選択された数から生成される。そのために、マイクロプロセッサ付カードは、必要な規模の整数を与えることができる、乱数の生成装置を有する。
したがって、図３には、本発明による方法を実施することができるマイクロプロセッサ付カードのフローチャートが示されている。

【００１６】

カードＣは、処理用メインユニット１と、ユニット１に連結されたプログラムメモリ３及び４と、作業メモリ（ここには記されていない）を備える。このカードはまた、モジュラ計算を行うことができる算術プロセッサ２と、一次性が検証された候補ｑが保存される安全化メモリ６（外部からはアクセスできない）を備える。このカードは、さらに、乱整数の生成装置５を有する。
とりわけ、上述したようなマイクロプロセッサカードでこの方法が実施されることを考慮すると、この方法によって実施される処理（算術プロセッサ２によって実施される演算）の速度を高め、作業メモリ内の場所を解放することが望ましい。

【００１７】

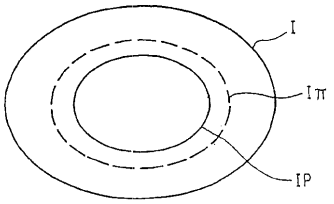
その目的で、ａ＝２を選択し、数Πから２を除外することによって（Π＝３，５，７，・・・）、モジュラ計算をしないで済ますことができる。実際、ｃの修正は２ｃ ｍｏｄ Π となる。ところが、ｃは Z^*_Π の要素であるから、２ｃ ｍｏｄ Π＝２ｃまたは２ｃ－

Πとなる。
しかし、このとき、新しい候補ｑは偶数である可能性もある。その場合には、新しい候補が常に集合ＩΠに属しながらも奇数になるような数をその新しい候補に加える。こうして、以下のようになる。
$\Pi = (\varepsilon_M - 1) \cdot \eta$
$q = c + \rho$
ｑが偶数である場合には、ｑはｑ＋ηとなる。
別の代案によれば、最初に定義したようなΠをそのままにし、ａがΠをともなう素数となるようなａの独自の値を選択することもできる。たとえば、$a = 2^{16} + 1$を選択することができる。

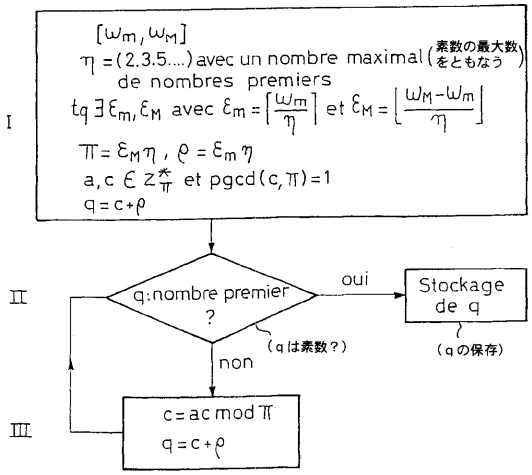
【００１８】
本発明による方法は、８ビットのＣＰＵと１１００ビットの暗号プロセッサを備えたInfeneonのチップカードＳＬＥ６６ＣＸ１６０Ｓのプラットフォームで実施された。ηとΠとρについては、以下の値が選択された。
η=b16bd1e084af628fe5089e6dabd16b5b80f60681d6a092fcb1e86d82876ed71921000bcfdd063fb90f81dfd07a021af23c735d52e63bd1cb59c93cbb398afd$_{16}$,
Π＝１７２９・η
ρ＝４１８０・η
ａ＝２とすると、４秒以内に５１２ビットの素数が得られる。したがって、平均して８秒以内に１０２４ビットの素数を得ることができる。

【図面の簡単な説明】
【図１】　区間［w_m、w_M］内に含まれる整数の集合Ｉと、互いに素のｋの区間の整数の集合ＩΠと、さらにこの区間の素数の集合ＩＰを示す図である。
【図２】　本発明による方法のフローチャートである。
【図３】　本発明による方法を実施するためのチップカードのような携帯電子装置の原理図である。

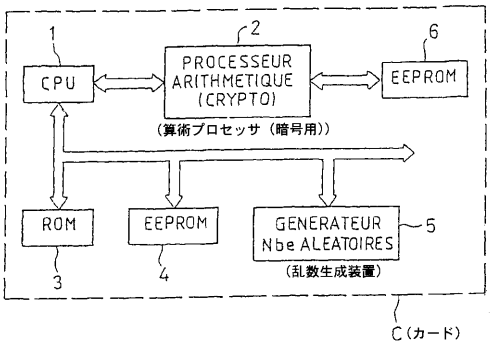
【図１】


I
Iπ
IP

【図２】


I
[ωm, ωM]
η = (2.3.5....) avec un nombre maximal de nombres premiers
(素数の最大数をともなう)
tq ∃εm, εM avec εm = ⌈ωm/η⌉ et εM = ⌊(ωM−ωm)/η⌋
π = εMη , ρ = εmη
a, c ∈ Z*π et pgcd(c, π)=1
q = c+ρ
II
q:nombre premier ?
(qは素数?)
oui
Stockage de q
(qの保存)
non
III
c = ac mod π
q = c+ρ

【図３】


1
CPU
2
PROCESSEUR ARITHMETIQUE (CRYPTO)
(算術プロセッサ（暗号用))
6
EEPROM
ROM
3
EEPROM
4
GENERATEUR Nbe ALEATOIRES
(乱数生成装置)
5
C(カード)

フロントページの続き

審査官　石田　信行

(56)参考文献　特開２０００－１２２５３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C 1/00