(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4649040号
(P4649040)
(45)発行日　平成23年3月9日(2011.3.9)　(24)登録日　平成22年12月17日(2010.12.17)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
G09C 1/00 (2006.01)　G09C 1/00 640B

請求項の数 17　(全 10 頁)

(21)出願番号　特願2000-519973(P2000-519973)
(86)(22)出願日　平成10年11月10日(1998.11.10)
(65)公表番号　特表2001-523067(P2001-523067A)
(43)公表日　平成13年11月20日(2001.11.20)
(86)国際出願番号　PCT/CA1998/001040
(87)国際公開番号　WO1999/025092
(87)国際公開日　平成11年5月20日(1999.5.20)
審査請求日　平成17年11月10日(2005.11.10)
(31)優先権主張番号　08/966,702
(32)優先日　平成9年11月10日(1997.11.10)
(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　オンタリオ　エル４ダブリュー　５エル１，ミシソーガ，エクスプローラー・ドライブ　５５２０，フォース・フロア
(74)代理人　100107489
弁理士　大塩　竹志
(74)代理人　100113701
弁理士　木島　隆一
(74)代理人　100115026
弁理士　圓谷　徹

最終頁に続く

(54)【発明の名称】マスクディジタル署名

(57)【特許請求の範囲】
【請求項１】
公開鍵データ通信システム内で、メッセージｍに署名し、前記メッセージｍを認証する方法であって、前記方法は、前記通信システムの装置によって実行され、前記装置は、長期秘密鍵ｄと、前記長期秘密鍵ｄから得られる対応する長期公開鍵とを有し、
前記方法は、
前記装置の安全なコンピュータシステムにおいて、
（ａ）第一の短期秘密鍵ｋを生成するステップと、
（ｂ）前記第一の短期秘密鍵ｋから得られる第一の短期公開鍵を計算するステップと、
（ｃ）前記第一の短期公開鍵を用いて第一の署名要素ｒを計算するステップと、
（ｄ）第二の短期秘密鍵ｔを生成するステップと、
（ｅ）前記メッセージｍに対する前記第二の短期秘密鍵ｔと、前記長期秘密鍵ｄと、前記第一の署名要素ｒとを用いて、第二の署名要素ｓを計算するステップと、
（ｆ）前記第一の短期秘密鍵ｋと前記第二の短期秘密鍵ｔとを用いて第三の署名要素ｃを計算し、前記署名要素（ｒ，ｓ，ｃ）を前記メッセージｍのマスクされたディジタル署名として前記装置の前記安全なコンピュータシステムに関連付けられた受信者側のコンピュータシステムに送信するステップと、
（ｇ）前記受信者側のコンピュータシステムが、前記第二および第三の署名要素（ｓ，ｃ）を用いて正規の署名要素ｓ－（ｓ－は、上線付きのｓを示す）を計算し、前記受信者側のコンピュータシステムが、前記署名要素（ｓ－，ｒ）を正規のディジタル署名として

前記公開鍵データ通信システムを介して受信者に送信するステップと
を含み、
前記受信者が前記正規のディジタル署名を受信し、検証することが可能である、方法。
【請求項２】
前記第一の短期秘密鍵ｋは、整数であり、
前記第一の短期公開鍵は、値ｋＰ＝（x_1，y_1）を計算することによって得られ、Ｐは、Ｅ（F_q）における素数の次数ｎの点であり、Ｅは、F_qに対して定義される楕円曲線である、請求項１に記載の方法。
【請求項３】
前記第一の署名要素ｒは、ｒ＝ｘ－（ｍｏｄ　ｎ）によって定義され、ｘ－（ｘ－は、上線付きのｘを示す）は、前記座標x_1を整数ｘ－に変換することによって得られる、請求項２に記載の方法。
【請求項４】
前記第二の短期秘密鍵ｔは、２≦ｔ≦（ｎ－２）を満たすように選択された整数であり、
前記第二の署名要素は、ｓ＝ｔ（ｅ＋ｄｒ）（ｍｏｄ　ｎ）によって定義され、ｅは、前記メッセージｍのハッシュである、請求項３に記載の方法。
【請求項５】
前記第三の署名要素は、ｃ＝ｔｋ（ｍｏｄ　ｎ）によって定義される、請求項４に記載の方法。
【請求項６】
前記正規な署名要素ｓ－は、$s^- = c^{-1}s \mod n$によって定義される、請求項５に記載の方法。
【請求項７】
データ通信システムにおいて、メッセージｍのディジタル署名Ｓを生成する方法であって、前記メッセージｍの署名者は、長期秘密鍵ｄと、前記長期秘密鍵ｄから得られる対応する長期公開鍵Ｑとを有し、前記方法は、
（ａ）短期秘密鍵ｋを生成するステップと、
（ｂ）前記短期秘密鍵ｋから得られる第一の短期公開鍵を計算するステップと、
（ｃ）前記第一の短期公開鍵を用いて第一の署名要素ｒを計算するステップと、
（ｄ）第二の短期秘密鍵ｔを生成するステップと、
（ｅ）前記メッセージｍに対する前記第二の短期秘密鍵ｔと、前記長期秘密鍵ｄと、前記第一の署名要素ｒとを用いて、第二の署名要素ｓを計算するステップと、
（ｆ）前記第一の短期秘密鍵ｋと前記第二の短期秘密鍵ｔとを用いて第三の署名要素ｃを計算するステップと、
（ｇ）前記署名要素（ｒ，ｓ，ｃ）を前記メッセージｍのマスクされたディジタル署名として受信者側のコンピュータシステムに送信するステップと、
（ｈ）前記受信者側のコンピュータシステムが、前記第二および第三の署名要素（ｓ，ｃ）を用いて正規の署名要素ｓ－（ｓ－は、上線付きのｓを示す）を計算し、前記受信者側のコンピュータシステムが、前記署名要素（ｓ－，ｒ）を正規のディジタル署名として検証者側のコンピュータシステムに送信し、前記正規のディジタル署名（ｓ－，ｒ）を前記検証者側のコンピュータシステムによって検証するステップと
を含む、方法。
【請求項８】
長期秘密鍵と、前記長期秘密鍵から得られる長期公開鍵と、体における所定の次数の生成元とを含まず、かつ、逆変換演算を行うことなく、暗号化ユニット内で、メッセージｍを署名する処理手段であって、前記処理手段は、
第一の短期秘密鍵を生成する生成器と、
第二の短期秘密鍵を生成する生成器と、
少なくとも前記第二の短期秘密鍵を用いて第一の署名要素を生成する生成器と

を含み、
前記処理手段は、前記メッセージｍの複数のマスクされた署名要素を生成するために、前記第一および第二の短期秘密鍵を用いて１つのマスクされた署名要素を生成するように動作し、
前記処理手段は、
前記署名要素を正規のディジタル署名要素に変換する変換器と、
前記正規のディジタル署名要素を受信者に送信するための通信チャネルと
をさらに含み、
前記受信者は、前記正規のディジタル署名を検証することが可能である、処理手段。
【請求項９】
送信者と受信者との間で確立されたデータ通信システムにおいて、メッセージｍの署名を検証する方法であって、前記送信者は、マスクされた署名要素（ｒ，ｓ，ｃ）を生成し、ｒは、第一の短期公開鍵ｋＰの座標から得られる第一の署名要素であり、ｓは、第二の短期秘密鍵と、前記メッセージｍと、長期秘密鍵と、前記第一の署名要素ｒとを結びつけることによって得られる第二の署名要素であり、ｃは、第一の短期秘密鍵および前記第二の短期秘密鍵を組み合わせることによって取得される第三の署名要素であり、前記方法は、
前記受信者が、
（ａ）署名要素のペア（ｓ－，ｒ）を取得するステップであって、前記要素ｓ－は、前記送信者によって生成された前記第二および第三の署名要素から得られる、ステップと、
（ｂ）前記署名要素のペア（ｓ－，ｒ）と前記メッセージｍとを用いて、前記第一の短期公開鍵ｋＰに対応する座標ペア（x_1，y_1）を復元するステップと、
（ｃ）前記座標ペアの１つから署名要素ｒ’を計算するステップと、
（ｄ）ｒ’＝ｒの場合、前記署名を検証するステップと
を含む、方法。
【請求項１０】
送信者と受信者との間で確立されたデータ通信システムにおいて、メッセージｍの署名を検証する方法であって、前記送信者は、マスクされた署名要素（ｒ，ｓ，ｃ）を生成し、ｒは、第一の短期公開鍵ｋＰの座標から得られる第一の署名要素であり、ｓは、第二の短期秘密鍵と、前記メッセージｍと、長期秘密鍵と、前記第一の署名要素ｒとを結びつけることによって得られる第二の署名要素であり、ｃは、第一の短期秘密鍵および前記第二の短期秘密鍵を組み合わせることによって取得される第三の署名要素であり、前記方法は、
前記送信者が、（ｒ，ｓ，ｃ）を署名要素のペア（ｓ－，ｒ）に変換し、前記送信者が、前記署名要素のペア（ｓ－，ｒ）を前記受信者に送信するステップと、
前記受信者が、
（ａ）前記署名要素のペア（ｓ－，ｒ）を取得するステップであって、前記要素ｓ－は、前記送信者によって生成された前記第二および第三の署名要素から得られる、ステップと、
（ｂ）前記署名要素のペア（ｓ－，ｒ）と前記メッセージｍとを用いて、前記第一の短期公開鍵ｋＰに対応する座標ペア（x_1，y_1）を復元するステップと、
（ｃ）前記座標ペアの１つから署名要素ｒ’を計算するステップと、
（ｄ）ｒ’＝ｒの場合、前記署名を検証するステップと
を含む、方法。
【請求項１１】
前記座標ペア（ｘ１，ｙ１）がｕおよびｖの値のペアを用いて計算され、前記ｕおよびｖの値は前記署名要素のペア（ｓ－，ｒ）および前記メッセージｍから得られる、請求項９に記載の方法。
【請求項１２】
前記座標ペア（x_1，y_1）は（x_1，y_1）＝ｕＰ＋ｖＱによって計算され、Ｐは、

楕円曲線Ｅ上の点であり、Ｑは、Ｑ＝ｄＰであるＰから得られる前記送信者の公開検証鍵である、請求項１１に記載の方法。

【請求項１３】

前記ｕの値は、ｕ＝ｓ－$^{-1}$ｅ　ｍｏｄ　ｎによって計算され、前記ｖの値は、ｖ＝ｓ－$^{-1}$ｒ　ｍｏｄ　ｎによって計算され、ｅは、前記メッセージｍのハッシュである、請求項１１に記載の方法。

【請求項１４】

ｅは、ｅ＝Ｈ（ｍ）によって計算され、Ｈ（）は前記送信者のハッシュ関数であり、かつ、前記受信者によって既知である、請求項１３に記載の方法。

【請求項１５】

前記座標x_1は、前記要素ｒ’の計算よりも前に、最初に整数（x_1）－（（x_1）－は、上線付きのx_1を示す）に変換される、請求項９に記載の方法。

【請求項１６】

前記要素ｒ’は、ｒ’＝（x_1）－　ｍｏｄ　ｎによって計算される、請求項１５に記載の方法。

【請求項１７】

前記要素ｒ’の計算よりも前に、前記座標ペア（x_1，y_1）が最初に検証され、前記座標ペア（x_1，y_1）が無限遠の点である場合、前記署名が拒絶される、請求項９に記載の方法。

【発明の詳細な説明】

本発明は、安全な通信システムに用いられるディジタル署名演算、特に計算能力の限られたプロセッサに用いられるディジタル署名演算を加速する方法に関するものである。

【０００１】

〔発明の背景〕

暗号システムの機能の一つとして、ディジタル署名の計算が挙げられる。ディジタル署名は、メッセージを作成したのが特定の人物であり、また該メッセージが通信中に変更されていないことを確認するのに用いられる。広く使用されている署名プロトコルは、送信者の秘密鍵でメッセージに署名するＥｌＧａｍａｌ公開鍵署名方式を用いている。また、受信者は、送信者の公開鍵でそのメッセージを復元することができる。ＥｌＧａｍａｌ方式では、有限体において離散対数を計算することでセキュリティを確保している。さらに、ＥｌＧａｍａｌタイプの署名は、不特定の群だけでなく特定の楕円曲線群においてもその役割を果たす。例えば、Ｅ（P_q）を楕円曲線群とし、Ｐ∈Ｅ（F_q）およびＱ＝ａＰとすると、離散対数の問題は整数ａを求めることに集約(reduce)される。従って、これらの暗号システムの計算は、集約的(intensive) である。

【０００２】

上記方式を実施する多数のプロトコルが存在する。例えば、ディジタル署名アルゴリズムＤＳＡは、ＥｌＧａｍａｌ方式の変形例である。このような方式においては、一組の通信者ＡおよびＢの各々が、公開鍵とそれに対応する秘密鍵とを生成する。通信者Ａは、任意の長さを有するメッセージｍに署名をし、通信者Ｂは、Ａの公開鍵を用いて該署名を検証する。しかしながら、送信者である通信者Ａにおいては署名の生成のために、受信者である通信者Ｂにおいては署名の検証のために、それぞれ集約的な計算の演算処理を行うことが必要であり、両者とも集約的な計算の演算処理を行うことが必要である。これは、通信者Ａおよび通信者Ｂの両者が十分な計算能力を持っている場合、特に問題とはならないが、通信者Ａおよび通信者Ｂの一方あるいは両者が、例えば“スマートカード”アプリケーションのような限られた計算能力しか持たない場合、これらの演算は、署名プロセスおよび検証プロセスに遅延を生じる。

【０００３】

公開鍵方式は、離散対数問題が難解と思われる多数の乗法群の中の一つを用いて実現できるが、有限体内での楕円曲線上の点の特徴を用いると、特に強固に実現できる。このような実現には、例えばＺｐ*で実現した場合と比べて、比較的低い次数の体(field) で必要

なセキュリティが得られるので、署名の通信に必要な帯域を狭くすることができるという利点がある。

【０００４】

楕円曲線ディジタル署名アルゴリズム（ＥＣＤＳＡ）等のディジタル署名アルゴリズムの一般的な実現において、署名要素ｓは

$s = k^{-1}(e + dr) \bmod n$

となる。ここで、ｄは署名者の長期秘密鍵としてのランダムな整数であり、Ｑは点Ｑ＝ｄＰの計算により得られる署名者の公開鍵であり、Ｐはシステムの予め定義されたパラメータである曲線上の点（ｘ，ｙ）であり、ｋは短期秘密鍵、すなわち短期セッション鍵として選択されるランダムな整数であり、かつ、対応する短期公開鍵Ｒ＝ｋＰを有し、ｅはメッセージのＳＨＡ－１ハッシュ関数等の安全ハッシュであり、ｎは曲線の次数である。

【０００５】

該方式では、署名者は点ｋＰのｘ座標を整数ｚとして表し、第一の署名要素$r = z \bmod n$を計算する。次に、上記の第二の署名要素ｓを計算し、署名要素ｓ、ｒとメッセージＭとを受信者へ送信する。受信者はＭ上の署名（ｒ，ｓ）を検証するために署名者の公開鍵Ｑを検索する。また、メッセージＭのハッシュｅ’を、ｅ’＝Ｈ（Ｍ）となるハッシュ関数Ｈを用いて計算する。さらに、値$c = s^{-1} \bmod n$も計算する。次に、$u_1 = e'c \bmod n$および$u_2 = rc \bmod n$となる整数値u_1およびu_2を計算する。署名を検証するには、値$u_1 P + u_2 Q$を計算しなくてはならない。Ｐは既知であり、システムワイドパラメータであるので、値$u_1 P$は迅速に計算できる。点$R = u_1 P + u_2 Q$を計算する。点Ｒ＝（x_1，ｙ）の体の要素ｘを整数ｚに変換し、値$v = z \bmod n$を計算する。ここで、ｖ＝ｒであれば、署名は妥当である。

【０００６】

ＭＱＶプロトコル等のその他のプロトコルも、楕円曲線上で実施される場合には同様の計算を必要とし、その結果、計算能力が限られている場合には署名および検証に時間がかかる。計算の複雑性は、楕円曲線の形の観察により説明される。一般に、基本楕円曲線は$y^2 + xy = x^3 + ax + b$であり、座標（x_1，y_1）の点と座標（x_2，y_2）の点とを加算し、点（x_3，y_3）を得る。ここでは、次式のようになる。

【０００７】

【数１】

$$x_3 = \left\{\left(\frac{y_1 \oplus y_2}{x_1 \oplus x_2}\right)^2 \oplus \frac{y_1 \oplus y_2}{x_1 \oplus x_2} \oplus x_1 \oplus x_2 \oplus a \right\} \quad (P \neq Q)$$

$$y_3 = \left\{\left(\frac{y_1 \oplus y_2}{x_1 \oplus x_2}\right) \oplus (x_1 \oplus x_3) \oplus x_3 \oplus y_1 \right\} \quad (P \neq Q)$$

【０００８】

点の倍加、つまりＰを２Ｐにすることは、点をそれ自身に足し合わせることによって行われ、次式のようになる。

【０００９】

【数２】

$$y_3 = \left\{x_1^2 \oplus \left(x_1 \oplus \frac{y_1}{x_1}\right)\right\} x_3 \oplus x_3$$

$$x_3 = x_1^2 \oplus \frac{b}{x_1^2}$$

【００１０】
上記ＥＣＤＳＡアルゴルズムの例から分かるように、第二の署名要素の計算では、少なくとも逆数(inverse) の計算が必要である。
【００１１】
ある数を法として、各倍点を生成するには、ｘおよびｙ両座標の計算が必要であり、ｙ座標の計算にはさらなる逆変換(inversion) が必要である。これらのステップは、複雑な計算であり、膨大な時間あるいは計算能力が要求される。
【００１２】
逆変換は、集約的な計算であり、通常、計算能力の限られた安全な境界内で実施される。このため、このような計算が境界外で実施できれば有利であり、計算能力が容易に得られる場合は特に有利である。しかしながら、この方法をＥＣＤＳＡ署名方式に直接適用すると、秘密鍵情報の信頼性を損なう可能性がある。そこで、既存の署名方式の安全レベルを維持しながら、署名演算の少なくとも一部を安全な境界外で実施することができる方法が必要とされている。
【００１３】
〔発明の概要〕
本発明の目的は、上記の不利益の少なくとも幾つかを軽減する方法および装置を提供することにある。
【００１４】
本発明は、“スマートカード”等の処理能力の限られたプロセッサにおいて、比較的効率的に実施可能なディジタル署名方法を提供する。
【００１５】
本発明は、全般的に署名の検証を加速する方法および装置を提供する。
【００１６】
本発明によれば、公開鍵データ通信システム内で、長期秘密鍵ｄと前記長期秘密鍵ｄから得られる長期公開鍵との対応によって、メッセージｍに署名し、前記メッセージｍを認証する方法であって、前記方法は、
安全なコンピュータシステムにおいて、
（ａ）第一の短期秘密鍵ｋを生成するステップと、
（ｂ）前記第一の短期秘密鍵ｋから得られる第一の短期公開鍵を計算するステップと、
（ｃ）前記第一の短期公開鍵を用いて第一の署名要素ｒを計算するステップと、
（ｄ）第二の短期秘密鍵ｔを生成するステップと、
（ｅ）前記第二の短期秘密鍵ｔと、長期秘密鍵と、第一の署名要素ｒとを用いて、第二の署名要素ｓを計算するステップと、
（ｆ）前記第一の短期秘密鍵ｋと前記第二の短期秘密鍵ｔとを用いて第三の署名要素ｃを計算し、前記署名要素（ｒ，ｓ，ｃ）を前記メッセージｍのマスクされたディジタル署名として前記安全なコンピュータシステムに関連付けられた受信者側のコンピュータシステムに送信するステップと、
（ｇ）前記第二および第三の署名要素（ｓ，ｃ）を用いて正規の署名要素ｓ－（ｓ－は、上線付きのｓを示す）を計算し、前記署名要素（ｓ－，ｒ）を正規のディジタル署名として前記公開鍵データ通信システム上で送信するステップと
を含み、
（ｈ）これにより、前記署名の受信者が前記正規のディジタル署名を検証することを可能にする、方法が提供される。
【００１７】
また、本発明によれば、安全な境界内に含まれる長期秘密鍵と、前記秘密鍵から得られる長期公開鍵と、体における所定の次数の生成元とを含まず、かつ、逆変換演算を行うことなくメッセージｍを署名する処理手段であって、前記処理手段は、
第一の短期秘密鍵を生成する生成器と、
第二の短期秘密鍵を生成する生成器と、

少なくとも前記第二の短期秘密鍵を用いて第一の署名要素を生成する生成器と
を含み、
前記処理手段は、前記メッセージｍの複数のマスクされた署名要素を生成するために、前記第一および第二の短期秘密鍵を用いて１つのマスクされた署名要素を生成するように動作する、処理手段が提供される。

【００１８】

〔好ましい実施形態の詳細な説明〕

図１に示すように、データ通信システム１０は、送信者１２および受信者１４の一組の通信者を含んでいる。送信者１２と受信者１４とは、互いに通信チャネル１６により接続されている。送信者１２および受信者１４はそれぞれ、ディジタル情報を処理するとともに通信チャネル１６を介した通信に備えてディジタル情報を用意する後述の暗号化ユニット１８および２０を有している。送信者はメッセージｍに署名し、該署名は受信者によって検証される。署名は、通常、暗号機１８において行われ、安全な境界として定義される。送信者は“スマートカード”、端末、あるいは同等の機器である。例えば、署名者が“スマートカード”である場合、その処理能力は限られている。しかしながら、“スマートカード”は、少なくともある程度の計算能力の備わった端末２２と接続して使用されるのが普通である。“スマートカード”は端末２２に挿入され、端末２２は“スマートカード”１２から受け取ったディジタル情報をチャネル１６を介して受信者１４へ送信する。端末は、該情報をチャネル１６を介して送信する前に、該情報に対し前処理を施しておいてもよい。

【００１９】

一般的な実施の形態では、送信者は、送信者の公開鍵Ｑ、メッセージｍ、送信者の短期公開鍵Ｒ、および送信者の署名Ｓ等を含むデータ列を組み立てる。データ列は、組み立てられると、意図された受信者１８へチャネル１６を介して送信される。署名Ｓは、通常一つ以上の要素から構成される。この点については、以下に、上記データ通信システムにより実施される署名方式に係る具体例を挙げて説明する。

【００２０】

本発明は、秘密鍵をマスクしてマスク署名要素を生成し、該マスク署名要素を署名の検証に先立ち正規署名へ変換する署名アルゴリズム全般について記述する。

【００２１】

図２に示すように、ＥをＦｑに対して定義される楕円曲線とし、ＰをＥ（F_q）上の素数の次数(prime order) ｎの点とし、ｄを２≦ｄ≦ｎ－２とする送信者の秘密署名鍵とし、Ｑ＝ｄＰを送信者の公開署名鍵とし、ｍを署名が施されるメッセージとする。さらに、これらのパラメータは、安全な境界内の、ブロック３０で示されるメモリ内に格納されているものとする。例えば、送信者が“スマートカード”の場合、“スマートカード”が安全な境界と定義され、また、例えば“スマートカード”が端末に挿入されている場合、端末が安全な境界外となる。送信者側での第一のステップはメッセージｍに署名することである。送信者は、メッセージｍのハッシュ値ｅ＝Ｈ（ｍ）（Ｈは、通常、ＳＨＡ－１ハッシュ関数である）を計算する。２≦ｋ≦（ｎ－２）となる第一の統計上特異で予測不可能な整数ｋ、つまり第一の短期秘密鍵を選択する。次に、点（x_1，y_1）＝ｋＰを計算する。点ｋＰの体(field) の要素x_1を整数x_1－（x_1－は、上線付きのx_1を表す）に変換し、第一の署名要素ｒ＝x_1－（ｍｏｄ　ｎ）を計算する。２≦ｔ≦（ｎ－２）となる第二の統計上特異で予測不可能な整数、つまり第二の短期秘密鍵を選択する。第二の署名要素ｓ＝ｔ（ｅ＋ｄｒ）（ｍｏｄ　ｎ）および第三の署名要素ｃ＝ｔｋ（ｍｏｄ　ｎ）を上記と同様に計算する。これにより、要素（ｒ，ｓ，ｃ）を有するマスクＥＣＤＳＡ署名が生成される。該マスクＥＣＤＳＡ署名（ｒ，ｓ，ｃ）を、ｓ－＝c^{-1}ｓ　ｍｏｄ　ｎを計算することによって、正規ＥＣＤＳＡ署名（ｓ－，ｒ）へ変換してもよい。この場合、送信者１２のＥＣＤＳＡ署名は、ｓ－とｒとである。署名（ｓ－，ｒ）は、後述の方法により正規ＥＣＤＳＡ署名として検証される。従って、送信者は、検証者が検証演算の前に変換演算を実施して署名（ｓ－，ｒ）を得ることができる場合にマスクＥＣＤＳＡ署名（

ｓ，ｒ，ｃ）を検証者へ送信してもよいし、例えば端末等の安全な境界外で上記変換を自身で行い、ＤＳＡ署名（ｓ－，ｒ）を検証者へ送信してもよい。

【００２２】

署名要素（ｓ－，ｒ）を受け取ると、受信者は、署名を検証するためにハッシュ値ｅ＝Ｈ（ｍ）（この場合、署名者のハッシュ関数はメッセージｍの検証者に既知である）を計算し、$u = s^{-1} e \mod n$および$v = s^{-1} r \mod n$を計算する。これにより、点（x_1，y_1）＝ｕＰ＋ｖＱが計算される。（x_1，y_1）が無限大の点である場合、該署名は拒否される。そうでなければ、体の要素x_1を整数x_1－に変換する。最後に、値ｒ’＝x_1－・ｍｏｄ　ｎを計算する。ここで、ｒ’＝ｒならば署名が承認（認証）され、ｒ’≠ｒならば署名は拒否される。

【００２３】

従って、マスクＥＣＤＳＡの利点は、マスク署名演算において、通常のＥＣＤＳＡで行われる法逆変換演算(modular inverse operation) を省略できることにある。前述のように、この利点は、特に、計算能力の限られているある種のアプリケーションには有益である。マスク署名のＥＣＤＳＡ署名への変換演算は、送信者の秘密鍵を保護している安全な境界の外で実施される。例えば、送信者がカード・リーダ（読み取り機）と通信する“スマートカード”の場合、該演算は“スマートカード”リーダ内で実施される。あるいは、マスク署名を検証者へ送信し、検証者が署名検証の前に変換演算を行ってもよい。マスクＥＣＤＳＡにおいては、ｔの選択に関わらず、必ず$t = ck^{-1}$となる。ここで、ｃはすでに公開されているので、ｔは独立した変数とはならない。

【００２４】

本発明をその具体例と特定の使用について説明したが、当業者ならば、添付の請求項に記載される発明の精神から逸脱することなく種々の変更が可能であろう。例えば、上記の好ましい実施の形態においては、乗法表記を使用していたが、本発明の方法は、加法表記でも同様に記述できる。例えば、ＥＣＤＳＡにおいて実施される楕円曲線アルゴリズムは、ＤＳＡと等価であり、また、離散対数アルゴリズムの楕円曲線のアナログ（相似形）は、通常F^*_pの集合体、つまり素数を法とする整数の乗法群によって記述されることは公知である。群F^*_pの要素および演算と、楕円曲線群Ｅ（F_q）との間には、対応関係がある。さらに、本署名技術は、F_pおよびF_{2^n}（$_{2^n}$は、下付き添字の2^nを表す）上で定義される体において実施される関数に対しても同様に適用可能である。また、上記ＤＳＡ署名方式は、公知であるＥｌＧａｍａｌ一般化(generalized) 署名方式の特異な事例であるので、本技術は、ＥｌＧａｍａｌ一般化署名方式にも適用可能である。

【００２５】

本発明は、暗号化方法および暗号化システム、特に有限体の要素をプロセッサにより効率的に掛け合わせてゆく楕円曲線暗号化方法および楕円曲線暗号化システム一般に関するものである。上記暗号化システムは、事前に好適にプログラムされた汎用コンピュータなどの、好適なプロセッサから構成されてもよい。

【図面の簡単な説明】

本発明の実施の形態は、次の添付図面を参照しながら説明する。

【図１】　通信システムを示す概略図である。

【図２】　本発明に係る署名アルゴリズムを示すフローチャートである。

【図１】

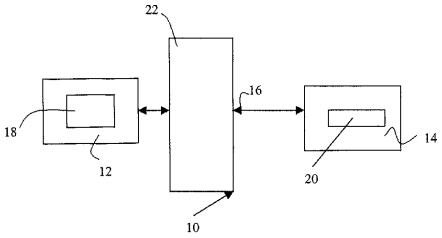
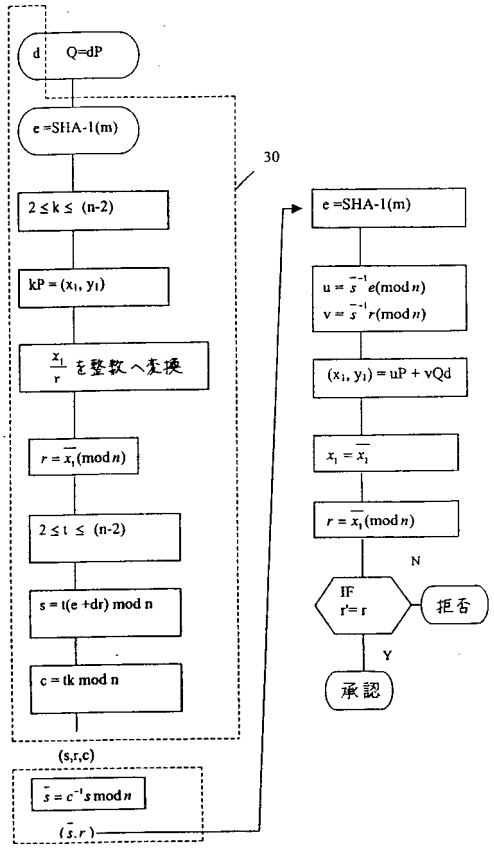


Figure 1

【図２】



フロントページの続き

(72)発明者 ヴァンストーン，スコット
カナダ，オンタリオ州 エル０ピー １ビー０，キャンベルヴィレ ピー．オー．ボックス ４９０ パインビュー トレイル １０１４０
(72)発明者 ジョンソン，ドナルド ビー．
アメリカ合衆国，ヴァージニア州 ２２０３３，フェアファックス，スリーピー レイク ドライブ ４２５３
(72)発明者 クー，ミンファ
カナダ，オンタリオ州 エル５エム ５ジー７，ミシソーガ ミドルベリ ドライブ ５４９５

審査官 新田 亮

(56)参考文献 特開平０９－１６０４９２（ＪＰ，Ａ）
欧州特許出願公開第０８０７９０８（ＥＰ，Ａ２）
Don B.Johnson, Elliptic Curve DSA(ECDSA):An Enhanced DSA, Proceedings of the 7th conference on USENIX Security Symposium, １９９８年, p.1-11, ＵＲＬ, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.5065

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
G09C 1/00