(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-506362
(P2017-506362A)
(43)公表日　平成29年3月2日(2017.3.2)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00 (2006.01)		G09C	1/00	620Z	5J104

審査請求 有　予備審査請求 未請求　（全 22 頁）

(21)出願番号　特願2016-548618 (P2016-548618)
(86)(22)出願日　平成27年1月30日 (2015.1.30)
(85)翻訳文提出日　平成28年7月27日 (2016.7.27)
(86)国際出願番号　PCT/US2015/013736
(87)国際公開番号　WO2015/116918
(87)国際公開日　平成27年8月6日 (2015.8.6)
(31)優先権主張番号　14/170,436
(32)優先日　平成26年1月31日 (2014.1.31)
(33)優先権主張国　米国 (US)

(71)出願人　502208397
グーグル　インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン　ビュー　アンフィシアター　パークウェイ　１６００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　ヤング，マーセル・エム・エム
アメリカ合衆国、９４０４３　カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００、グーグル・インコーポレイテッド内

最終頁に続く

(54)【発明の名称】関連付けられた秘密鍵部分を用いた高速公開鍵暗号化のためのシステムおよび方法

(57)【要約】
関連付けられた秘密鍵部分を用いた高速公開鍵暗号化のためのシステムおよび方法が記載されており、当該システムおよび方法は、平文を暗号文に暗号化するステップを含み、暗号化するステップは、公開鍵と、対応する秘密鍵とを使用し、当該システムおよび方法はさらに、暗号文を格納するステップを含む。

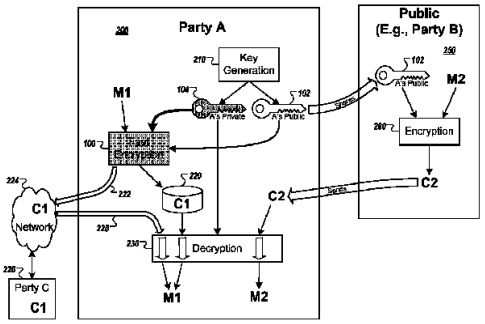

FIG. 2

【特許請求の範囲】
【請求項１】
コンピュータによって実行される方法であって、
平文を暗号文に暗号化するステップを備え、前記暗号化するステップは、公開鍵と、対応する秘密鍵とを使用し、前記方法はさらに、
前記暗号文を格納するステップを備える、方法。
【請求項２】
前記公開鍵は、合成数ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、ｎ＝ｐ×ｑである、請求項１に記載の方法。
【請求項３】
前記対応する秘密鍵を使用する前記暗号化するステップは、ｇ１およびｇ２を使用するステップを備え、前記ｇ１は、前記ｐに関連付けられる巡回群の生成元であり、前記ｇ２は、前記ｑに関連付けられる巡回群の生成元である、請求項２に記載の方法。
【請求項４】
前記対応する秘密鍵を使用する前記暗号化するステップは、ＧＮ１およびＧＮ２を使用するステップをさらに備え、前記ＧＮ１は、前記ｇ１に基づく定数であり、前記ＧＮ２は、前記ｇ２に基づく定数である、請求項３に記載の方法。
【請求項５】
前記平文を前記暗号化するステップは、ｓ１およびｓ２を使用するステップをさらに備え、前記ｓ１は、前記ｐに基づく乱数であり、前記ｓ２は、前記ｑに基づく乱数である、請求項２に記載の方法。
【請求項６】
【数１】

前記平文を前記暗号化するステップは、前記ｓ１、前記ｓ２および中国剰余定理を用いて値ｒを算出するステップをさらに備え、$r \in \mathbb{Z}^*_{n^2}$である、請求項５に記載の方法。

【請求項７】
デジタル署名照合のためのコンピュータによって実行される方法であって、
秘密鍵を用いてデジタル署名されるメッセージに基づいて照合結果を生成するステップを備え、前記生成するステップは、前記秘密鍵と、対応する公開鍵とを使用し、前記方法はさらに、
前記照合結果を格納するステップを備える、方法。
【請求項８】
前記公開鍵は、合成数Ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、Ｎ＝ｐ×ｑである、請求項７に記載の方法。
【請求項９】
コンピュータによって実行可能な命令を格納した非一時的なコンピュータ読取可能な媒体であって、前記命令は、
平文を暗号文に暗号化するためのものであり、前記暗号化は、公開鍵と、対応する秘密鍵とを使用し、前記命令はさらに、
前記暗号文を格納するためのものである、コンピュータ読取可能な媒体。
【請求項１０】
前記公開鍵は、合成数ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、ｎ＝ｐ×ｑである、請求項９に記載のコンピュータ読取可能な媒体。
【請求項１１】
前記対応する秘密鍵を使用する前記暗号化は、ｇ１およびｇ２を使用することを備え、前記ｇ１は、前記ｐに関連付けられる巡回群の生成元であり、前記ｇ２は、前記ｑに関連付けられる巡回群の生成元である、請求項１０に記載のコンピュータ読取可能な媒体。

【請求項１２】
前記対応する秘密鍵を使用する前記暗号化は、ＧＮ１およびＧＮ２を使用することをさらに備え、前記ＧＮ１は、前記ｇ１に基づく定数であり、前記ＧＮ２は、前記ｇ２に基づく定数である、請求項１１に記載のコンピュータ読取可能な媒体。
【請求項１３】
前記平文の前記暗号化は、ｓ１およびｓ２を使用することをさらに備え、前記ｓ１は、前記ｐに基づく乱数であり、前記ｓ２は、前記ｑに基づく乱数である、請求項１０に記載のコンピュータ読取可能な媒体。
【請求項１４】
【数２】

前記平文の前記暗号化は、前記ｓ１、前記ｓ２および中国剰余定理を用いて値ｒを算出することをさらに備え、$r \in \mathbb{Z}^*_{n^2}$である、請求項１３に記載のコンピュータ読取可能な媒体。

【請求項１５】
記憶装置とプロセッサとを備える少なくとも１つのコンピュータ装置であって、前記プロセッサは、
平文を暗号文に暗号化することを実行するように構成されており、前記暗号化は、公開鍵と、対応する秘密鍵とを使用し、前記プロセッサはさらに、
前記暗号文を格納することを実行するように構成されている、少なくとも１つのコンピュータ装置。
【請求項１６】
前記公開鍵は、合成数ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、ｎ＝ｐ×ｑである、請求項１５に記載の少なくとも１つのコンピュータ装置。
【請求項１７】
前記対応する秘密鍵を使用する前記暗号化は、ｇ１およびｇ２を使用することを備え、前記ｇ１は、前記ｐに関連付けられる巡回群の生成元であり、前記ｇ２は、前記ｑに関連付けられる巡回群の生成元である、請求項１６に記載の少なくとも１つのコンピュータ装置。
【請求項１８】
前記対応する秘密鍵を使用する前記暗号化は、ＧＮ１およびＧＮ２を使用することをさらに備え、前記ＧＮ１は、前記ｇ１に基づく定数であり、前記ＧＮ２は、前記ｇ２に基づく定数である、請求項１７に記載の少なくとも１つのコンピュータ装置。
【請求項１９】
前記平文の前記暗号化は、ｓ１およびｓ２を使用することをさらに備え、前記ｓ１は、前記ｐに基づく乱数であり、前記ｓ２は、前記ｑに基づく乱数である、請求項１６に記載の少なくとも１つのコンピュータ装置。
【請求項２０】
【数３】

前記平文の前記暗号化は、前記ｓ１、前記ｓ２および中国剰余定理を用いて値ｒを算出することをさらに備え、$r \in \mathbb{Z}^*_{n^2}$である、請求項１９に記載の少なくとも１つのコンピュータ装置。

【発明の詳細な説明】
【技術分野】
【０００１】
分野
本明細書に記載されている主題は、一般にデータ処理に関し、より特定的には、関連付

けられた秘密鍵部分を用いた高速公開鍵暗号化のためのシステムおよび方法に関する。
【背景技術】
【０００２】
関連背景
公開鍵暗号化または非対称暗号化では、暗号システムは、３つのアルゴリズムで構成されており、すなわち、所有者によって維持される秘密鍵および所有者によって公衆に公開される公開鍵を生成する鍵生成のための１つのアルゴリズム、公開された公開鍵にアクセスできる誰もが公開鍵を用いて暗号化を行うことができるようにする暗号化のための１つのアルゴリズム、および、秘密鍵または「トラップドア」情報を有する所有者が、公開鍵を用いて暗号化された秘密鍵データにより復号化を行うことができるようにする復号化のための１つのアルゴリズムである。
【０００３】
例えばＲＳＡ（リベスト・シャミア・エーデルマン）アルゴリズムでは、秘密鍵も公開鍵も２つの素数を用いて生成される。所有者は、２つの素数を知っており、当該素数を用いて復号化を行うことができる。「公衆」（すなわち、２つの素数の合成体の少なくとも何らかの形態に基づいて公開鍵を提供されるもの）は、公開鍵を用いて暗号化を行うことができる。公衆は、事実上、当該合成体を因数分解することはできず、復号化を行うことはできない。
【０００４】
特定のシナリオでは、暗号化を行うパーティは、秘密鍵の所有者でもある。例えば、所有者は、データを暗号化してパブリックネットワークを通じて送信したい、および／または、第三者ストレージ（例えば、クラウドストレージ）に格納したい場合がある。暗号化されたデータは、後に抽出されて、所有者によって復号化され得る。
【発明の概要】
【課題を解決するための手段】
【０００５】
概要
主題は、関連付けられた秘密鍵部分を用いた高速公開鍵暗号化のための方法を含み、当該方法は、平文を暗号文に暗号化するステップを含み、暗号化するステップは、公開鍵と、対応する秘密鍵とを使用し、当該方法はさらに、暗号文を格納するステップを含む。
【０００６】
当該方法は、１つ以上のコンピュータ装置および／またはシステムを用いて実現される。当該方法は、コンピュータ読取可能な媒体に格納されてもよい。
【図面の簡単な説明】
【０００７】
【図１】高速暗号化実現例のハイレベル図を示す。
【図２】高速暗号化実現例を配備することができる例示的な環境を示す。
【図３】プロセス実現例の一例を示す。
【図４】いくつかの例示的な実現例に適した例示的な環境を示す。
【図５】いくつかの例示的な実現例での使用に適した例示的なコンピュータ装置を有する例示的なコンピュータ環境を示す。
【発明を実施するための形態】
【０００８】
詳細な説明
本明細書に記載されている主題は、例示的な実現例によって教示される。明確にするため、および主題を曖昧にすることを回避するために、さまざまな詳細は省略されている。以下に示される例は、関連付けられた秘密鍵部分を用いた高速公開鍵暗号化のためのシステムおよび方法を実現するための構造および機能に向けられる。
【０００９】
図１は、高速暗号化実現例のハイレベル図を示す。例示的な高速暗号化１００は、公開

鍵１０２の少なくとも一部と、対応する秘密鍵１０４（復号鍵と呼ぶことができる）の少なくとも一部とを用いて、データまたはメッセージＭを暗号化して暗号文Ｃを生成するように実現される。高速暗号化１００は、公開鍵１０２の少なくとも一部を用いて暗号化を行うために１つ以上のアルゴリズムを実行するソフトウェアモジュール、プロセス、ソフトウェアアプリケーション、ハードウェア回路、物理的装置、またはこれらの任意の組み合わせであってもよい。

【００１０】

高速暗号化１００は、公開鍵などと秘密鍵などとを使用する任意の暗号システムにおいて、暗号化、認証、デジタル署名などのために実現され得る。本明細書に記載されている技術を用いて高速化可能な例示的なアルゴリズムは、トランスポート層セキュリティ（Transport Layer Security：ＴＬＳ）、プリティ・グッド・プライバシ（Pretty Good Privacy：ＰＧＰ）、リベスト・シャミア・エーデルマン（Rivest, Shamir and Adleman：ＲＳＡ）、準同型暗号（例えば、Paillier暗号）などを含むが、これらに限定されるものではない。アルゴリズムは、（例えば、ディフィー・ヘルマン鍵交換などを用いた）鍵配布または秘密鍵配布を含み得る。

【００１１】

以下の図２に記載されているように、暗号文Ｃは、公開鍵１０２のみを用いてデータを暗号化する従来の暗号化アルゴリズムを用いて暗号化された別の暗号文Ｃ２と同等であり得る。言い換えれば、同一の復号エンジンが暗号文Ｃおよび暗号文Ｃ２を復号化することができ、高速暗号化アルゴリズム１００を用いてＣが暗号化されるか、従来の暗号化アルゴリズムを用いてＣが暗号化されるかを区別することはできない。

【００１２】

図２は、高速暗号化実現例を配備することができる例示的な環境を示す。パーティＡ２００（例えば、所有者）は、鍵生成２１０を用いて公開鍵１０２と秘密鍵１０４（または、復号鍵１０４）とを生成する。鍵生成１２０は、鍵を生成するために１つ以上のアルゴリズムを実行するソフトウェアモジュール、プロセス、ソフトウェアアプリケーション、ハードウェア回路、物理的装置、またはこれらの任意の組み合わせであってもよい。公開鍵１０２は、暗号化されたメッセージを所有者２００に送りたい任意のパーティ（例えば、パーティＢ２５０）に提供され得る。所有者２００は、秘密鍵１０４を用いて、公開鍵１０２により暗号化されたメッセージを復号する。また、所有者２００は、１つ以上の高速暗号化または高速認証アルゴリズムにおいて秘密鍵１０４または秘密鍵１０４の少なくとも一部を用いる。

【００１３】

【数１】

鍵生成２１０は、例えば２つの素数ｐおよびｑをランダムに互いに独立して計算または選択することによって鍵（例えば、公開鍵１０２および秘密鍵１０４）を生成する。実現例は、同等の長さ（例えば、２５６ビット、５１２ビット、１０２４ビット、２０４８ビット、2^Xではない長さなど）の素数ｐおよびｑを使用してもよい。ｇｃｄ（ｐｑ，（ｐ－１）（ｑ－１））＝１の特性を検証するために、最大公約数（すなわち、ｇｃｄ）が計算され得る。公開鍵（例えば、公開鍵１０２）を生成するために、鍵生成２１０は、ｎ＝ｐｑを計算し、ｇ＝ｎ＋１などの乱数整数ｇを選択し、$g \in \mathbb{Z}^*n^2$、$\mathbb{Z}^*n^2 = \{ i \in \mathbb{Z} : 1 \leq i \leq (n^2-1) \text{ and } gcd(i, n^2) = 1 \}$、および$\mathbb{Z}n^2 = \{0, 1, \cdots, (n^2-1)\}$である。公開鍵は、（ｎ，ｇ）である。公開鍵は、ｐおよびｑを取得するために事実上解読または因数分解できない合成数ｎを含む。ｐおよび／またはｑが大きくなればなるほど（例えば、ビットの長さが長くなればなるほど）、ｎを解読することが困難になる。

本明細書に記載されている例では、式$c = (g^m)(r^n) \bmod n^2$を用いて平文ｍを暗号文ｃに暗号化することができ、$m \in \mathbb{Z}n$であり、ｒはランダムに選択され、$r \in \mathbb{Z}^*n$または$r \in \mathbb{Z}^*n^2$である。$\mathbb{Z}n = \{0, 1, \cdots, (n-1)\}$であり、$\mathbb{Z}^*n = \{ i \in \mathbb{Z} : 1 \leq i \leq (n-1) \text{ and } gcd(i, n) = 1 \}$である。式$c = (g^m)(r^n) \bmod n^2$は、ＥＱ１として参照され得る。本明細書における「平文」または「ｍ」（例えば、図１に示されるＭならびに図２に示されるＭ１およびＭ２）という用語は、暗号化されるデータ、情報またはメッセージを指す。「平文」または「ｍ」は、人間が読み取れる形態もしくはマシンが解読できる形態であってもよく、または、人間が読み取ることができない形態もしくはマシンが解読できない形態（例えば、前もって暗号化された形態）であってもよい。

【００１４】

復号化を行う所有者またはパーティのみが、ｐおよびｑを知っているまたは知っているべきである。ｐおよびｑが分かっていると、秘密鍵を容易に生成することができる。対応する秘密鍵（例えば、公開鍵１０２を用いて暗号化された暗号文を復号化するための秘密鍵１０４）を生成するために、鍵生成２１０は、$\lambda = lcm(p-1, q-1)$を計算し、ｌｃｍは最小公倍数である。また、鍵生成２１０は、$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$を計算し、$L(\mu) = (\mu-1)/n$である。秘密（復号）鍵は、（λ，μ）である。本明細書に記載されている例における復号化式は、$m = L(c^{\lambda} \bmod n^2)\mu \bmod n$である。

【００１５】

秘密鍵（例えば、λおよびμ）を生成する別の例示的な方法は、ｐおよびｑが同等の長さを有する場合、$\lambda = \Phi(n) = (p-1)(q-1)$、$\mu = \Phi(n)^{-1} \bmod n$およびｇ＝ｎ＋１を計算することによるものである。

【００１６】

例えば、ｐおよびｑは、５１２ビットの長さの数であってもよく、結果として生じるｎは、１０２４ビットの長さの合成数であってもよい。ｐおよびｑが１０２４ビットの長さの素数であれば、その結果として、ｎは２０４８ビットの長さであってもよい（この合成体は「ＲＳＡ数」と呼ばれる）。

【００１７】

復号化を行う所有者またはパーティのみがｐおよびｑを知っているまたは知っているべきであるので、所有者（例えば、所有者のコンピュータ装置またはシステム）のみがｐおよび／またはｑを用いて暗号化を行うことができる。高速暗号化１００は、例えば、秘密鍵１０４または秘密鍵の構成要素（例えば、ｐおよびｑ）を用いて暗号化を加速させるように実現される。

【００１８】

図１に示されるように、高速暗号化１００は、公開鍵１０２と対応する秘密鍵１０４（またはその一部）とを両方とも用いてデータ（例えば、メッセージＭ１）を暗号化して、暗号文（例えば、暗号文Ｃ１）を生成する。

【００１９】

ＥＱ１暗号化式は、$c=(g^m)(r^n) \mod n^2$である。ｇとしてｎ＋１が使用されると、暗号化式は、$c=((n+1)^m)(r^n) \mod n^2$になり、これは、$(n+1)^m \mod n^2$の２項展開により、$c=(1+nm)(r^n) \mod n^2$（ＥＱ２として参照され得る）に変化させることができる。ＥＱ２では、１つのべき乗（すなわち、g^m）が除去されており、計算時間を短縮することができる。ＥＱ２は、残りのべき乗（すなわち、r^n）を１つだけ有している。

【００２０】

ｐおよびｑを使用することによって、残りのべき乗を除去することができ、またはその計算時間を短縮することができる。基数が固定されて指数が変化する場合に、事前計算は高速になるであろう。ｐおよびｑを用いて暗号化を加速させる目的で（すなわち、これは、ｐおよびｑを知っているまたはｐおよびｑにアクセスできる秘密鍵１０４の所有者によってのみ行われることができる）、固定された基数で事前計算を行うことができるようにＥＱ２の「$(r^n) \mod n^2$」部分を変換するために、周知の中国剰余定理（Chinese Remainder Theorem：ＣＲＴ）が使用されてもよい。

【００２１】

【数２】

なお、$n^2=p^2q^2$である。n^2のｎ番目の剰余から乱数ｒを選択するオペレーションは、p^2のｎ番目の剰余から乱数ｒ１を選択し、q^2のｎ番目の剰余から乱数ｒ２を選択することに置き換えられてもよい。ＣＲＴを用いて、ｒ１およびｒ２を組み合わせて、p^2q^2またはn^2のｎ番目の剰余を得ることができる。ＣＲＴを用いて、$(r^n) \mod n^2=(r^n) \mod p^2q^2$は、乱数ｒ１およびｒ２について$(r1)^n \mod p^2$および$(r2)^n \mod q^2$に変換されることができ、$(r1)(r2)=r$、$r1 \in \mathbb{Z}^*p^2$、および$r2 \in \mathbb{Z}^*q^2$である。

位数$\Phi(p^2)$の巡回群$\mathbb{Z}^*p^2$の生成元ｇ１を選択し、$\Phi(p^2)$から乱数要素ｓ１を選択し、$y1=(g1)^{s1} \mod p^2$を計算することによって、ｒ１の値はランダムに選択されることができる。$\Phi(p^2)$は、オイラーのファイ関数であり、p^2と互いに素であるp^2未満の正の整数（すなわち、１，２，...，(p^2-1)）の数である。

位数$\Phi(q^2)$の巡回群$\mathbb{Z}^*q^2$の生成元ｇ２を選択し、$\Phi(q^2)$から乱数要素ｓ２を選択し、$y2=(g2)^{s2} \mod q^2$を計算することによって、ｒ２の値はランダムに選択され得る。$\Phi(q^2)$は、オイラーのファイ関数であり、q^2と互いに素であるq^2未満の正の整数（すなわち、１，２，...，(q^2-1)）の数である。

【００２２】

ｎ番目の剰余を取得するために、ｙ１およびｙ２はｎ乗に累乗される。したがって、$(y1)^n=[(g1)^{s1} \mod p^2]^n=[(g1)^{s1}]^n \mod p^2=(g1^n)^{s1} \mod p^2$であり、$(y2)^n=[(g2)^{s2} \mod q^2]^n=[(g2)^{s2}]^n \mod q^2=(g2^n)^{s2} \mod q^2$である。参考までに、$g1^n \mod p^2$は、ＧＮ１として参照され得て、$g2^n \mod q^2=GN2$である。その結果、固定ベースのＧＮ１は、乱数$s1 \mod p^2$の指数に累乗され（すなわち、$GN1^{s1} \mod p^2$）、固定ベースのＧＮ２は、乱数$s2 \mod q^2$の指数に累乗される（すなわち、$GN2^{s2} \mod q^2$）。

【００２３】

高速暗号化１００は、一度値を事前計算し、ｐおよびｑの各組み合わせについて一度だけ値を事前計算する。説明を簡単にするために、一例として小さなｐおよびｑの値が選択される。コンピュータ装置またはシステムによる実際の実現例では、ｐおよびｑの値は、

２５６ビットであってもよく、５１２ビットであってもよく、１０２４ビットであってもよく、２０４８ビットであってもよく、または他のビット数の長さであってもよい。例えば、以下に示される例では、ｐ＝５であり、ｑ＝７である。上記の例示的な実現例は、以下の一連の演算に示されるようにｐおよびｑの値に適用される。

【００２４】

【数３】

ｐ＝５、p^2＝２５

$\mathbb{Z}^*p^2$＝（１，２，３，４，６，７，８，９，１１，１２，１３，１４，１６，１７，１８，１９，２１，２２，２３，２４）

Φ（p^2）＝$\mathbb{Z}^*p^2$のサイズ＝２０

p^2のｇ１＝｛１：１，２：２０，３：２０，４：１０，５：２，６：５，７：４，８：２０，９：１０，１０：２，１１：５，１２：２０，１３：２０，１４：１０，１５：２，１６：５，１７：２０，１８：４，１９：１０，２０：２，２１：５，２２：２０，２３：２０，２４：２｝であり、最高次は２０である。生成元ｇ１は、（２，３，８，１２，１３，１７，２２，または２３）であってもよい。

例えば、ｇ１＝２である。

ｑ＝７、q^2＝４９

$\mathbb{Z}^*q^2$＝（１，２，３，４，５，６，８，９，１０，１１，１２，１３，１５，１６，１７，１８，１９，２０，２２，２３，２４，２５，２６，２７，２９，３０，３１，３２，３３，３４，３６，３７，３８，３９，４０，４１，４３，４４，４５，４６，４７，４８）

Φ（q^2）＝$\mathbb{Z}^*q^2$のサイズ＝４２

q^2のｇ２＝｛１：１，２：２１，３：４２，４：２１，５：４２，６：１４，７：２，８：７，９：２１，１０：４２，１１：２１，１２：４２，１３：１４，１４：２，１５：７，１６：２１，１７：４２，１８：３，１９：６，２０：１４，２１：２，２２：７，２３：２１，２４：４２，２５：２１，２６：４２，２７：１４，２８：２，２９：７，３０：３，３１：６，３２：２１，３３：４２，３４：１４，３５：２，３６：７，３７：２１，３８：４２，３９：２１，４０：４２，４１：１４，４２：２，４３：７，４４：２１，４５：４２，４６：２１，４７：４２，４８：２｝であり、最高次は４２である。生成元ｇ２は、（３，５，１０，１２，１７，２４，２６，３３，３８，４０，４５，または４７）であってもよい。

例えば、ｇ２＝３である。

ｎ＝ｐｑ＝３５、n^2＝35^2＝１２２５

$GN1=g1^n \mod p^2=2^{35} \mod 25=18$

$GN2=g2^n \mod q^2=3^{35} \mod 49=19$

【００２５】

上記の定数値を事前計算した後、高速暗号化１００は、例えば以下のアルゴリズムを用いて任意のデータまたはメッセージｍを暗号文ｃに暗号化することができる。

【００２６】

ＥＱ２は、ｃ＝（１＋ｎｍ）（r^n） ｍｏｄ n^2であり、「（r^n） ｍｏｄ n^2」部分は、$GN1^{s1} \mod p^2$および$GN2^{s2} \mod q^2$に対するＣＲＴ（中国剰余定理）を用いて計算されることができる。

【００２７】

Ｄ＝（１＋ｎｍ） ｍｏｄ n^2とする。したがって、Ｄの計算は、基本的には、（例えば、時間および／またはリソース消費量の点で）計算コストが最も高いという観点から、１回の乗算である。

【００２８】

実行されたように乱数要素ｓ１をΦ（ｐ^{2}）から選択し、乱数要素ｓ２をΦ（ｑ^{2}）から選択するオペレーションは、計算コストの観点では取るに足らない。

【００２９】

Ｅ＝ＧＮ１^{s1}　ｍｏｄ　ｐ^{2}およびＦ＝ＧＮ２^{s2}　ｍｏｄ　ｑ^{2}を計算する。計算コストは、基本的には、固定基数による２つのべき乗演算である。固定基数べき乗は、加法鎖、特にピッペンジャのべき乗アルゴリズム（Pippenger's Exponentiation Algorithm）の方法によって加速させることができる。

【００３０】

高速暗号化１００は、ＣＲＴを用いて計算を実行し、ＥおよびＦを組み合わせて、結果Ｈ＝（ｒ^{n}）　ｍｏｄ　ｎ^{2}を生成する。計算コストは、いかなるべき乗演算も実行することを含んでいない。

【００３１】

次いで、高速暗号化１００は、ｃ＝ＤＨ　ｍｏｄ　ｎ^{2}を計算する。

例えば、図２に示されるように、高速暗号化１００は、メッセージＭ１を暗号化して、暗号文Ｃ１を生成し得る。Ｍ１＝１２（すなわち、ｍ＝１２）である。（ｐ＝５およびｑ＝７に基づいて）事前計算された定数ＧＮ１およびＧＮ２を用いて、高速暗号化１００は、以下を選択および／または計算する：

Ｄ＝（１＋ｎｍ）　ｍｏｄ　ｎ^{2}＝（１＋３５×１２）　ｍｏｄ　３５^{2}＝４２１

ｓ１＝７およびｓ２＝９（ランダムに選択される）

Ｅ＝ＧＮ１^{s1}　ｍｏｄ　ｐ^{2}＝１８^{7}　ｍｏｄ　２５＝７

Ｆ＝ＧＮ２^{s2}　ｍｏｄ　ｑ^{2}＝１９^{9}　ｍｏｄ　４９＝４８

Ｈは、以下の２つの式を用いて計算することができる

ｘ≡７　ｍｏｄ　２５

ｘ≡４８　ｍｏｄ　４９

Ｈ＝８３２

Ｃ１＝ＤＨ　ｍｏｄ　ｎ^{2}＝４２１×８３２　ｍｏｄ　１２２５＝１１４７。

【００３２】

【数４】

高速暗号化１００によって暗号化されるデータが、一度に暗号化可能な量よりも大きいまたは長い場合（例えば、ｍ　∈　ℤｎ）、当該データは、各セグメント　∈　ℤｎという条件を満たすようにセグメントに分割されることができる。結果として生じる暗号文は、連結可能である。逆のプロセスまたは復号化プロセスでは、連結された暗号文は、個々の平文に復号化される前に個々の暗号文に分割されることができる。平文は、元のデータを形成するように連結可能である。

【００３３】

高速暗号化１００がＭ１を暗号化してＣ１を作成した後、Ｃ１は、例えばパーティＡまたは所有者２００によって制御されるデータベース２２０に格納され得る。また、Ｃ１は、ネットワーク２２４（例えば、パブリックネットワークまたはインターネット）を介して、経路２２２を通って例えばパーティＣ２２６に送信され得る。パーティＣは、データ格納サービスを提供する第三者（例えば、クラウドストレージサービスプロバイダ）であってもよい。いくつかの実現例では、暗号文Ｃ１は、ネットワーク２２４を介して送信されて、パーティＡによって制御される装置またはシステム（図示せず）によって格納または処理され得る。パーティＡがＭ１またはＣ１の平文データにアクセスしたい場合、パーティＡは、データベース２２０に格納されていればデータベース２２０からＣ１を抽出してもよく、またはネットワーク２２４および経路２２８を介してパーティＣからＣ１を抽出してもよい。Ｃ１の供給源にかかわらず、パーティＡは、復号化エンジン２３０（または復号化２３０）を用いてＣ１を復号化することができる。

【００３４】

高速暗号化１００とは対照的に、公開鍵１０２にアクセスできる（すなわち、ｐおよびｑを知らない）パーティ（例えば、パーティＢ）のみが、公開鍵を用いて暗号化を行う。例えば、パーティＡ２００は、公開鍵１０２をパーティＢ２５０に提供して、パーティＢは、メッセージＭ２を暗号文Ｃ２に暗号化してパーティＡに送る。Ｍ２は、いかなる値であってもよい。パーティＢの暗号化エンジン２６０は、ＥＱ１ｃ＝（ｇ^{m}）（ｒ^{n}） ｍｏｄ ｎ^{2}を用いてＭ２を暗号化する。例えばｎ＝３５であり、例えばｇ＝３６である。パーティＢは、合成数ｎの因数ｐおよびｑを知らない。暗号化エンジン２６０は、上記のように乱数ｒを選択する。例えば、ｒ＝２３である。比較のために、Ｍ２＝１２（すなわち、ｍ＝１２）である。ＥＱ１は、Ｃ２＝（ｇ^{m}）（ｒ^{n}） ｍｏｄ ｎ^{2}＝（３６^{12}）（２３^{35}） ｍｏｄ １２２５＝５２２になる。パーティＢは、Ｃ２をパーティＡに送る。なお、ＥＱ１は、秘密鍵１０４（例えば、因数ｐおよびｑ）または値λおよび／もしくはμを使用しない。

【００３５】

パーティＡの復号化エンジン２３０は、Ｃ１（すなわち、秘密鍵１０４および公開鍵１０２を用いて高速暗号化１００によって暗号化される）およびＣ２（すなわち、公開鍵１０２だけを用いてパーティＢの暗号化エンジン２６０によって暗号化される）を同じように復号化することができる。Ｃ１およびＣ２が（例えば、別々に）いつ到達するかにかかわらず、Ｃ１およびＣ２は、同一の復号化鍵または秘密鍵１０４（例えば、λ、μ）を用いて独立して復号化される。

【００３６】

復号化のために、復号化エンジン２３０は、以下の値を抽出または計算する：

ｐ＝５、ｑ＝７、ｎ＝ｐｑ＝３５、ｎ^{2}＝１２２５

ｇ＝ｎ＋１＝３６

λ＝ｌｃｍ（ｐ－１，ｑ－１）＝１２

μ＝（Ｌ（ｇ$^{\lambda}$ ｍｏｄ ｎ^{2}））$^{-1}$ ｍｏｄ ｎ、ここで、Ｌ（ｕ）＝（ｕ－１）／ｎである

ｕ＝ｇ$^{\lambda}$ ｍｏｄ ｎ^{2}＝３６^{12} ｍｏｄ ３５^{2}＝４２１

Ｌ（ｕ）＝（４２１－１）／３５＝１２

μ＝（１２）$^{-1}$ ｍｏｄ ３５＝３

秘密鍵（λ，μ）＝（１２，３）

復号化式は、ｍ＝Ｌ（ｃ$^{\lambda}$ ｍｏｄ ｎ^{2}）μ ｍｏｄ ｎである

ｍ＝Ｌ（ｃ$^{\lambda}$ ｍｏｄ ｎ^{2}）μ ｍｏｄ ｎ＝（ｋ）μ ｍｏｄ ｎ、ここで、ｋ＝Ｌ（ｃ$^{\lambda}$ ｍｏｄ ｎ^{2}）であり、Ｌ（ｕ）＝（ｕ－１）／ｎである。

【００３７】

復号化エンジン２３０は、Ｃ１を復号化して平文Ｍ１を取得し、Ｃ２を復号化して平文Ｍ２を取得する。復号化エンジン２３０は、以下の値を計算して、Ｃ１（高速暗号化１００によって生成されたＣ１＝１１４７）を復号化する：

ｕ＝Ｃ１$^{\lambda}$ ｍｏｄ ｎ^{2}＝１１４７^{12} ｍｏｄ １２２５＝１４１

ｋ＝（１４１－１）／３５＝４

Ｍ１＝（ｋ）μ ｍｏｄ ｎ＝（４）３ ｍｏｄ ３５＝１２。

【００３８】

復号化エンジン２３０は、以下の値を計算して、Ｃ２（暗号化エンジン２６０によって生成されたＣ２＝５２２）を復号化する：

ｕ＝Ｃ２$^{\lambda}$ ｍｏｄ ｎ^{2}＝５２２^{12} ｍｏｄ １２２５＝１４１

ｋ＝（１４１－１）／３５＝４

Ｍ２＝（ｋ）μ ｍｏｄ ｎ＝（４）３ ｍｏｄ ３５＝１２。

【００３９】

Ｃ１が高速暗号化アルゴリズムを用いて暗号化され、Ｃ２が従来の暗号化アルゴリズムを用いて暗号化されることにかかわらず、同一の復号化エンジン２３０が暗号文Ｃ１およびＣ２を復号化することができる。

【００４０】
図３は、プロセス実現例の一例を示す。プロセス３００は、例えばブロック３１０を含み、ブロック３１０において、高速暗号化１００は、合成数ｎ＝ｐ×ｑ（例えば、公開鍵１０２）を用いてデータ（例えば、Ｍ１）を暗号文（例えば、Ｃ１）に暗号化し、ｐおよびｑは、素数であってもよい。暗号化オペレーションを加速させるために、高速暗号化１００は、秘密鍵１０４の構成要素であるｐおよびｑも個々に使用した。例えば、ｇ１およびＧＮ１は、ｐを用いてまたはｐに基づいて計算され、ｇ２およびＧＮ２は、ｑを用いてまたはｑに基づいて計算される。ブロック３２０において、暗号化されたデータ（例えば、Ｃ１）は、（例えば、データベース２２０に）格納されてもよく、または別の場所もしくはパーティ（例えば、パーティＣ）に送られてもよい。

【００４１】
いくつかの例では、プロセス３００は、異なるブロックにより実現されてもよく、より少ない数のブロックにより実現されてもよく、またはより多い数のブロックにより実現されてもよい。プロセス３００は、コンピュータによって実行可能な命令として実現されてもよく、当該命令は、媒体に格納され、１つ以上のコンピュータ装置の１つ以上のプロセッサにロードされ、コンピュータによって実行される方法として実行されてもよい。

【００４２】
公開鍵オペレーションにおいて秘密鍵を使用する別の例は、署名照合（例えば、デジタル署名を用いて署名されたメッセージまたはデータの真正性を確認すること）である。例えば、ＲＳＡ署名鍵を作成するために、整数ｅおよびｄとともに、２つの大きな素数（例えば、ｐおよびｑ）の積である係数Ｎを含むＲＳＡ鍵ペアを生成し、（ｅ）（ｄ）≡１（ｍｏｄ　Φ（Ｎ））であり、Φはオイラーのファイ関数である。署名者の公開鍵は、Ｎおよびｅで構成され、署名者の秘密鍵は、ｄを含む。

【００４３】
メッセージｍを署名するために、署名者は、$\sigma \equiv m^{d} \pmod{N}$を計算する。デジタル署名されたメッセージσを照合するために、受信者は、$\sigma^{e} \equiv m \pmod{N}$を確認する。素因数ｐおよびｑ（すなわち、秘密鍵）を保持するパーティは、ＲＳＡ署名照合を実行することができ、ＲＳＡ署名照合は、σをｅ乗に累乗する代わりに、ＣＲＴを用いて演算ｍｏｄ　ｐおよびｍｏｄ　ｑを実行して、上記のＥＱ２の「$(r^{n}) \bmod n^{2}$」部分の変換と同様のｅ乗　ｍｏｄ　Ｎへのメッセージの計算を加速させる。

【００４４】
【数５】

例えば、σをｅ乗　ｍｏｄ　合成体Ｎに累乗するオペレーションは、乱数ｒ１をｐのｎ番目の剰余から選択し、乱数ｒ２をｑのｎ番目の剰余から選択することに置き換えられてもよい。ＣＲＴを用いて、ｒ１およびｒ２を組み合わせて、ｐｑまたはＮのｅ番目の剰余を取得することができる。ＣＲＴを用いて、$(\sigma^{e}) \bmod N = (\sigma^{e}) \bmod pq$は、乱数ｒ１およびｒ２について$(r1)^{e} \bmod p$および$(r2)^{e} \bmod q$に変換されることができ、$(r1)(r2) = \sigma$、$r1 \in \mathbb{Z}^{*}p$、および$r2 \in \mathbb{Z}^{*}q$である。オペレーションは、上記のようにｒ１およびｒ２を計算した後も継続する。

【００４５】
同一のオペレーションは、因数（秘密鍵）を知っているパーティによるＲＳＡ暗号化のさらに別の例にも適用可能である。例えば、秘密鍵を用いてデジタル署名されたデータまたはメッセージを照合するために、当該メッセージに基づく照合結果が、（例えば、秘密鍵を知っているパーティによって）秘密鍵および対応する公開鍵の少なくとも一部を用いて生成されてもよい。照合結果は、例えば「照合済」である場合もあれば「却下」である場合もある。結果は、例えばログまたはデータベースに格納されてもよい。

【００４６】

図４は、いくつかの例示的な実現例に適した例示的な環境を示す。環境４００は、装置４０５～４４５を含み、各々は、例えばネットワーク４６０を介して（例えば、有線および／または無線接続によって）少なくとも１つの他の装置に通信可能に接続されている。いくつかの装置は、１つ以上の記憶装置４３０および４４５に通信可能に接続されてもよい。

【００４７】

１つ以上の装置４０５～４４５の一例は、図５における後述のコンピュータ装置５０５であってもよい。装置４０５～４４５は、コンピュータ４０５（例えば、ラップトップコンピュータ装置）、モバイル機器４１０（例えば、スマートフォンまたはタブレット）、テレビ４１５、車両４２０に関連付けられる装置、サーバコンピュータ４２５、コンピュータ装置４３５～４４０、記憶装置４３０および４４５を含み得るが、これらに限定されるものではない。

【００４８】

いくつかの実現例では、装置４０５～４２０は、ユーザ装置（例えば、クラウドストレージサービスプロバイダに格納されたデータなどのデータにアクセスするためにユーザによって使用される装置）であると考えられてもよい。装置４２５～４４５は、（例えば、サービスを提供するため、ならびに／または、暗号化されたウェブページ、テキスト、テキスト部分、画像、画像部分、音声、音声セグメント、映像、映像セグメント、および／もしくはそれらについての情報を格納するなどデータを格納するために、サービスプロバイダによって使用される）サービスプロバイダに関連付けられる装置であってもよい。

【００４９】

例えば、ユーザ（例えば、アリス）は、１つ以上の装置４２５～４４５によってサポートされるストレージプロバイダに暗号化されたデータを送るために装置４０５または４１０を使用してもよい。アリスは、秘密鍵を用いて当該データを暗号化することができ、計算時間および／またはリソースを節約する。暗号化されたデータは、ストレージプロバイダによって復号化されることはできない。アリスは、データにアクセスしたいときには、（例えば、暗号化された形態の）データをストレージプロバイダから抽出して、アリスの装置４０５または４１０上で当該データを復号化する。

【００５０】

図５は、いくつかの例示的な実現例での使用に適した例示的なコンピュータ装置を有する例示的なコンピュータ環境を示す。コンピュータ環境５００におけるコンピュータ装置５０５は、１つ以上の処理ユニット、コアもしくはプロセッサ５１０、メモリ５１５（例えば、ＲＡＭ、ＲＯＭなど）、内部ストレージ５２０（例えば、磁気ストレージ、光学式ストレージ、ソリッドステートストレージおよび／もしくはオーガニックストレージ）、ならびに／または、Ｉ／Ｏインターフェース５２５を含み得て、それらはいずれも、情報を通信するための通信機構またはバス５３０上で結合されてもよく、またはコンピュータ装置５０５に組み込まれてもよい。

【００５１】

コンピュータ装置５０５は、入力／ユーザインターフェース５３５および出力装置／インターフェース５４０に通信可能に結合されることができる。入力／ユーザインターフェース５３５および出力装置／インターフェース５４０のどちらか一方または両方は、有線または無線インターフェースであってもよく、着脱可能であってもよい。入力／ユーザインターフェース５３５は、入力を提供するために使用可能な、物理的なまたはバーチャルな任意の装置、構成要素、センサまたはインターフェース（例えば、ボタン、タッチスクリーンインターフェース、キーボード、ポインティング／カーソル制御装置、マイクロホン、カメラ、点字、モーションセンサ、光学式読取装置など）を含み得る。出力装置／インターフェース５４０は、ディスプレイ、テレビ、モニタ、プリンタ、スピーカ、点字などを含み得る。いくつかの例示的な実現例では、入力／ユーザインターフェース５３５および出力装置／インターフェース５４０は、コンピュータ装置５０５に組み込まれてもよく、またはコンピュータ装置５０５に物理的に結合されてもよい。他の例示的な実現例で

は、他のコンピュータ装置が、入力／ユーザインターフェース５３５および出力装置／インターフェース５４０として機能してもよく、または、入力／ユーザインターフェース５３５および出力装置／インターフェース５４０の機能をコンピュータ装置５０５に提供してもよい。

【００５２】

コンピュータ装置５０５の例としては、高モバイル機器（例えば、スマートフォン、車両および他のマシン内の装置、人間および動物によって携帯される装置など）、モバイル機器（例えば、タブレット、ノート型パソコン、ラップトップ、パーソナルコンピュータ、携帯型テレビ、ラジオなど）、および、移動させることを考えて設計されていない装置（例えば、デスクトップコンピュータ、他のコンピュータ、情報キオスク、１つ以上のプロセッサを組み込んだおよび／または結合させたテレビ、ラジオなど）を挙げることができるが、これらに限定されるものではない。

【００５３】

コンピュータ装置５０５は、外部ストレージ５４５と、同一または異なる構成の１つ以上のコンピュータ装置を含むさまざまなネットワーク化された構成要素、装置およびシステムと通信するためのネットワーク５５０とに（例えば、Ｉ／Ｏインターフェース５２５を介して）通信可能に結合されることができる。コンピュータ装置５０５または任意の接続されたコンピュータ装置は、サーバ、クライアント、シンサーバ、汎用マシン、特殊用途マシン、もしくは別のラベルとして機能するものであってもよく、サーバ、クライアント、シンサーバ、汎用マシン、特殊用途マシン、もしくは別のラベルのサービスを提供するものであってもよく、または、サーバ、クライアント、シンサーバ、汎用マシン、特殊用途マシン、もしくは別のラベルと呼ばれてもよい。

【００５４】

Ｉ／Ｏインターフェース５２５は、コンピュータ環境５００における少なくとも全ての接続された構成要素、装置およびネットワークに、および／または、コンピュータ環境５００における少なくとも全ての接続された構成要素、装置およびネットワークから情報を通信するための任意の通信またはＩ／Ｏプロトコルまたは規格（例えば、イーサネット（登録商標）、８０２．１１ｘ、ユニバーサルシステムバス、ワイマックス、モデム、セルラーネットワークプロトコルなど）を使用する有線および／または無線インターフェースを含み得るが、これらに限定されるものではない。ネットワーク５５０は、任意のネットワークまたはネットワークの組み合わせ（例えば、インターネット、ローカルエリアネットワーク、広域ネットワーク、電話ネットワーク、セルラーネットワーク、衛星ネットワークなど）であってもよい。

【００５５】

コンピュータ装置５０５は、一時的な媒体および非一時的な媒体を含むコンピュータによって使用可能なまたはコンピュータ読取可能な媒体を使用することができ、および／または、コンピュータによって使用可能なまたはコンピュータ読取可能な媒体を使用して通信することができる。一時的な媒体は、伝送媒体（例えば、金属ケーブル、光ファイバ）、信号、搬送波などを含む。非一時的な媒体は、磁気媒体（例えば、ディスクおよびテープ）、光媒体（例えば、ＣＤ　ＲＯＭ、デジタルビデオディスク、ブルーレイ（登録商標）ディスク）、ソリッドステート媒体（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリ、ソリッドステートストレージ）、および他の不揮発性記憶装置またはメモリを含む。

【００５６】

コンピュータ装置５０５は、いくつかの例示的なコンピュータ環境において技術、方法、アプリケーション、プロセス、またはコンピュータによって実行可能な命令を実行するために使用されることができる。コンピュータによって実行可能な命令は、一時的な媒体から抽出されてもよく、非一時的な媒体に格納されて非一時的な媒体から抽出されてもよい。実行可能な命令は、任意のプログラミング言語、スクリプト言語およびマシン言語（例えば、Ｃ、Ｃ＋＋、Ｃ＃、Ｊａｖａ（登録商標）、ビジュアルベーシック、パイソン、パール、ＪａｖａＳｃｒｉｐｔ（登録商標）など）のうちの１つ以上から生成されてもよ

い。

【００５７】

プロセッサ５１０は、ネイティブなまたはバーチャルな環境ではいかなるオペレーティングシステム（operating system：ＯＳ）（図示せず）下でも動作することができる。１つ以上のアプリケーションを配備することができ、当該１つ以上のアプリケーションは、論理ユニット５６０と、アプリケーションプログラミングインターフェース（application programming interface：ＡＰＩ）ユニット５６５と、入力ユニット５７０と、出力ユニット５７５と、事前計算エンジン５８０と、乱数発生器５８５と、暗号化エンジン５９０と、さまざまなユニットが互いに、ＯＳと、および他のアプリケーション（図示せず）と通信するようにするためのユニット間通信機構５９５とを含む。例えば、事前計算エンジン５８０、乱数発生器５８５および暗号化エンジン５９０は、図１～図４に示され記載されている１つ以上のプロセスを実行することができる。記載されているユニットおよび要素は、設計、機能、構成またはインプリメンテーションの点で変更可能であり、記載されている説明に限定されるものではない。

【００５８】

いくつかの例示的な実現例では、情報または実行命令は、ＡＰＩユニット５６５によって受取られると、１つ以上の他のユニット（例えば、論理ユニット５６０、入力ユニット５７０、出力ユニット５７５、事前計算エンジン５８０、乱数発生器５８５および暗号化エンジン５９０）に通信されることができる。例えば、入力ユニット５７０がメッセージＭを検出した後、入力ユニット５７０は、ＡＰＩユニット５６５を用いてメッセージＭを事前計算エンジン５８０に通信してもよい。事前計算エンジン５８０は、暗号化オペレーションで必要な定数および／または値が確実に利用可能であることを確認する。利用可能でなければ、事前計算エンジン５８０は、これらの定数および／または値を生成または事前計算する。次いで、事前計算エンジン５８０は、暗号化エンジン５９０を呼び出して、Ｍを暗号化する。暗号化エンジン５９０は、必要であれば乱数発生器５８５を呼び出して、暗号化に使用される乱数ｓ１およびｓ２を生成する。暗号化エンジン５９０がＭを暗号文Ｃに暗号化した後、暗号化エンジン５９０は、Ｃを出力ユニット５７５に渡し、出力ユニット５７５は、Ｃを格納するため、またはネットワークでＣを送信するためにｉ／ｏインターフェース５２５と対話することができる。

【００５９】

いくつかの例では、論理ユニット５６０は、上記のいくつかの例示的な実現例においてユニット間の情報フローを制御し、ＡＰＩユニット５６５、入力ユニット５７０、出力ユニット５７５、事前計算エンジン５８０、乱数発生器５８５および暗号化エンジン５９０によって提供されるサービスを仕向けるように構成されてもよい。例えば、１つ以上のプロセスまたは実現例のフローは、論理ユニット５６０単独で、またはＡＰＩユニット５６５とともに制御されてもよい。

【００６０】

いくつかの例示的な実現例を図示および説明してきたが、これらの例示的な実現例は、本明細書に記載されている主題をこの分野の当業者に伝えるために提供されている。本明細書に記載されている主題は、記載されている例示的な実現例に限定されることなく、さまざまな形態で実現されてもよいということが理解されるべきである。本明細書に記載されている主題は、それらの具体的に規定もしくは記載されている事項がなくても実施可能であり、または、記載されていない他のもしくは異なる要素もしくは事項とともに実施されてもよい。添付の特許請求の範囲およびそれらの等価物に規定されている本明細書に記載の主題から逸脱することなく、これらの例示的な実現例において変更を加え得ることは、この分野の当業者によって理解されるであろう。

【図３】

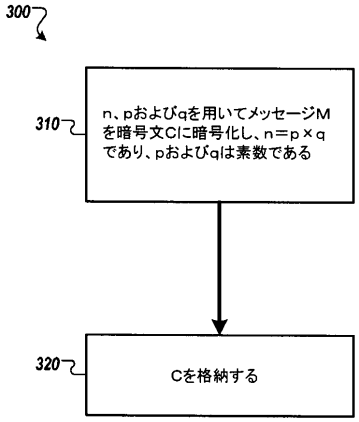

FIG. 3

【図４】

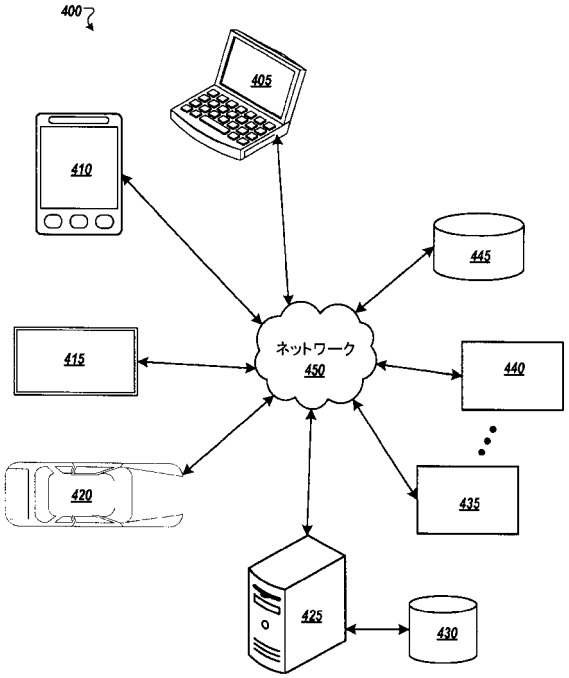

FIG. 4

【図５】

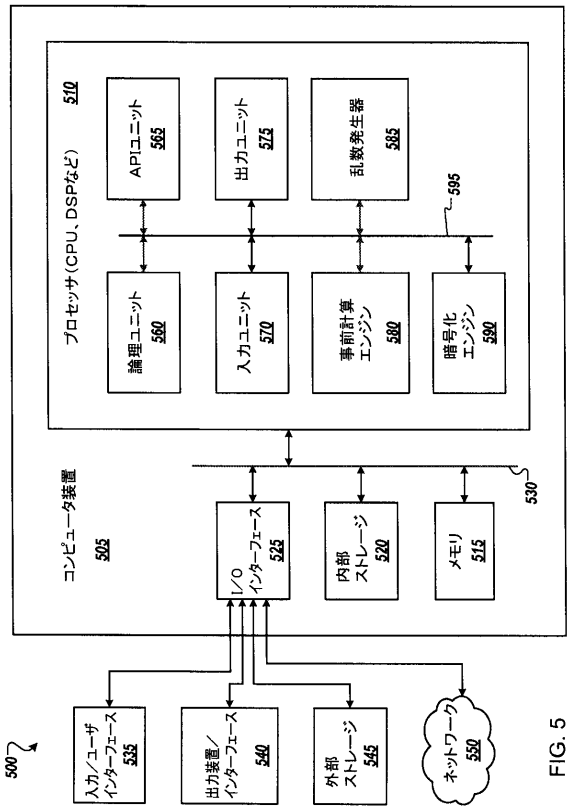

FIG. 5

【図１】

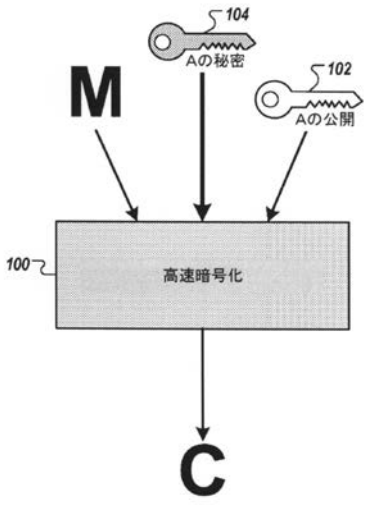

FIG. 1

【図２】

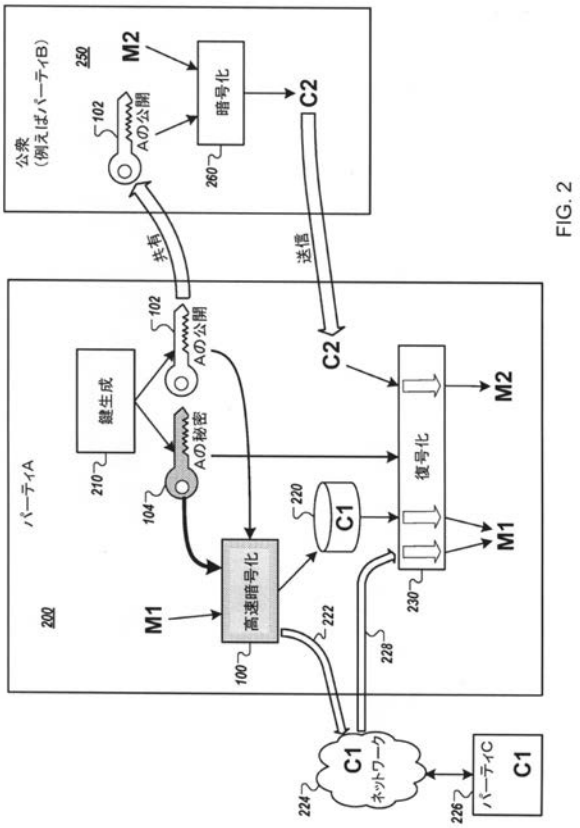

FIG. 2

【手続補正書】
【提出日】平成28年11月25日(2016.11.25)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピュータによって実行される方法であって、
平文を暗号文に暗号化するステップを備え、前記暗号化するステップは、公開鍵と、対応する秘密鍵とを使用し、前記方法はさらに、
前記暗号文を格納するステップを備える、方法。
【請求項２】
前記公開鍵は、合成数ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、ｎ＝ｐ×ｑである、請求項１に記載の方法。
【請求項３】
前記対応する秘密鍵を使用する前記暗号化するステップは、ｇ１およびｇ２を使用するステップを備え、前記ｇ１は、前記ｐに関連付けられる巡回群の生成元であり、前記ｇ２は、前記ｑに関連付けられる巡回群の生成元である、請求項２に記載の方法。
【請求項４】
前記対応する秘密鍵を使用する前記暗号化するステップは、ＧＮ１およびＧＮ２を使用するステップをさらに備え、前記ＧＮ１は、前記ｇ１に基づく定数であり、前記ＧＮ２は、前記ｇ２に基づく定数である、請求項３に記載の方法。
【請求項５】

前記平文を前記暗号化するステップは、ｓ１およびｓ２を使用するステップをさらに備え、前記ｓ１は、前記ｐに基づく乱数であり、前記ｓ２は、前記ｑに基づく乱数である、請求項２から４のいずれか１項に記載の方法。
【請求項６】
【数１】

前記平文を前記暗号化するステップは、前記ｓ１、前記ｓ２および中国剰余定理を用いて値ｒを算出するステップをさらに備え、ｒ　∈　$\mathbb{Z}^*_{n^2}$である、請求項５に記載の方法。

【請求項７】
デジタル署名照合のためのコンピュータによって実行される方法であって、
秘密鍵を用いてデジタル署名されるメッセージに基づいて照合結果を生成するステップを備え、前記生成するステップは、前記秘密鍵と、対応する公開鍵とを使用し、前記方法はさらに、
前記照合結果を格納するステップを備える、方法。
【請求項８】
前記公開鍵は、合成数Ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、Ｎ＝ｐ×ｑである、請求項７に記載の方法。
【請求項９】
コンピュータに方法を実行させるためのプログラムであって、前記方法は、
平文を暗号文に暗号化するステップを備え、前記暗号化は、公開鍵と、対応する秘密鍵とを使用し、前記方法はさらに、
前記暗号文を格納するステップを備える、プログラム。
【請求項１０】
前記公開鍵は、合成数ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、ｎ＝ｐ×ｑである、請求項９に記載のプログラム。
【請求項１１】
前記対応する秘密鍵を使用する前記暗号化するステップは、ｇ１およびｇ２を使用するステップを備え、前記ｇ１は、前記ｐに関連付けられる巡回群の生成元であり、前記ｇ２は、前記ｑに関連付けられる巡回群の生成元である、請求項１０に記載のプログラム。
【請求項１２】
前記対応する秘密鍵を使用する前記暗号化するステップは、ＧＮ１およびＧＮ２を使用するステップをさらに備え、前記ＧＮ１は、前記ｇ１に基づく定数であり、前記ＧＮ２は、前記ｇ２に基づく定数である、請求項１１に記載のプログラム。
【請求項１３】
前記平文を前記暗号化するステップは、ｓ１およびｓ２を使用するステップをさらに備え、前記ｓ１は、前記ｐに基づく乱数であり、前記ｓ２は、前記ｑに基づく乱数である、請求項１０から１２のいずれか１項に記載のプログラム。
【請求項１４】
【数２】

前記平文を前記暗号化するステップは、前記ｓ１、前記ｓ２および中国剰余定理を用いて値ｒを算出することをさらに備え、ｒ　∈　$\mathbb{Z}^*_{n^2}$である、請求項１３に記載のプログラム。

【請求項１５】
記憶装置とプロセッサとを備える少なくとも１つのコンピュータ装置であって、前記プロセッサは、
平文を暗号文に暗号化する手段を備え、前記暗号化する手段は、公開鍵と、対応する秘密鍵とを使用し、前記プロセッサはさらに、
前記暗号文を格納する手段を備える、少なくとも１つのコンピュータ装置。

【請求項１６】
前記公開鍵は、合成数ｎを備え、前記秘密鍵は、素数ｐおよびｑを用いて生成され、ｎ＝ｐ×ｑである、請求項１５に記載の少なくとも１つのコンピュータ装置。
【請求項１７】
前記対応する秘密鍵を使用する前記暗号化する手段は、ｇ１およびｇ２を使用する手段を備え、前記ｇ１は、前記ｐに関連付けられる巡回群の生成元であり、前記ｇ２は、前記ｑに関連付けられる巡回群の生成元である、請求項１６に記載の少なくとも１つのコンピュータ装置。
【請求項１８】
前記対応する秘密鍵を使用する前記暗号化する手段は、ＧＮ１およびＧＮ２を使用する手段をさらに備え、前記ＧＮ１は、前記ｇ１に基づく定数であり、前記ＧＮ２は、前記ｇ２に基づく定数である、請求項１７に記載の少なくとも１つのコンピュータ装置。
【請求項１９】
前記平文を前記暗号化する手段は、ｓ１およびｓ２を使用する手段をさらに備え、前記ｓ１は、前記ｐに基づく乱数であり、前記ｓ２は、前記ｑに基づく乱数である、請求項１６から１８のいずれか１項に記載の少なくとも１つのコンピュータ装置。
【請求項２０】
【数３】

前記平文を前記暗号化する手段は、前記ｓ１、前記ｓ２および中国剰余定理を用いて値ｒを算出する手段をさらに備え、$r \in \mathbb{Z}^*_{n^2}$である、請求項１９に記載の少なくとも１つのコンピュータ装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/013736

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Chapter 8: Public-Key Encryption ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 283 - 319 , 1 October 1996 (1996-10-01), XP001525008, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/	1-3,5, 7-11,13, 15-17,19
A	algorithm 8.1	4,6,12, 14,18,20
	----- -/--	

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
11 May 2015	19/05/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/013736

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	"Chapter 2: Mathematical Background ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 49 - 86 , 1 October 1996 (1996-10-01), XP001525002, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/ fact 2.120	
X	PAILLER P ED - STERN J (ED): "PUBLIC-KEY CRYPTOSYSTEMS BASED ON COMPOSITE DEGREE RESIDUOSITY CLASSES", 1 January 1999 (1999-01-01), ADVANCES IN CRYPTOLOGY - EUROCRYPT '99. INTERNATIONAL CONF. ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PRAGUE, CZ, MAY 2 - 6, 1999 PROCEEDINGS; [LECTURE NOTES IN COMPUTER SCIENCE], BERLIN : SPRINGER, DE, PAGE(S) 223 - 238, XP000830710, ISBN: 978-3-540-65889-4	1,2,5, 7-10,13, 15,16,19
A	the whole document section 4, scheme 1 section 7, decryption using CRT	6,14,20
A	US 2002/064278 A1 (LIM SEONGAM [KR] ET AL) 30 May 2002 (2002-05-30) paragraphs [0043] - [0056]; figure 2	1-20

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/013736

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002064278 A1	30-05-2002	KR 20010067016 A	12-07-2001
		US 2002064278 A1	30-05-2002

フロントページの続き

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

(72)発明者 パテール, サーバー
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００、グーグル・インコーポレイテッド内

Ｆターム(参考) 5J104 AA18 JA21 NA02 NA37 PA07