

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2018-142013

(P2018-142013A)

(43) 公開日 平成30年9月13日(2018.9.13)

(51) Int.Cl. F 1 テーマコード (参考)
G 0 9 C 1/00 (2006.01) G 0 9 C 1/00 6 2 0 Z 5 J 1 0 4

審査請求 有 請求項の数 6 O L 外国語出願 (全 19 頁)

(21) 出願番号	特願2018-90042 (P2018-90042)	(71) 出願人	502208397
(22) 出願日	平成30年5月8日 (2018.5.8)		グーグル エルエルシー
(62) 分割の表示	特願2016-548618 (P2016-548618) の分割		アメリカ合衆国 カリフォルニア州 94 043 マウンテン ビュー アンフィシ アター パークウェイ 1600
原出願日	平成27年1月30日 (2015.1.30)	(74) 代理人	110001195
(31) 優先権主張番号	14/170,436		特許業務法人深見特許事務所
(32) 優先日	平成26年1月31日 (2014.1.31)	(72) 発明者	ヤング, マーセル・エム・エム
(33) 優先権主張国	米国 (US)		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】 (修正有)

【課題】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、コンピュータ読取可能な媒体及びコンピュータ装置を提供する。

【解決手段】平文を暗号文に暗号化するステップと、暗号文を格納するステップを備える。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する。公開鍵は、合成数 n を備え、秘密鍵は、素数 p および q を用いて生成され、 $n = p \times q$ である。対応する秘密鍵を使用する暗号化するステップは、 g_1 および g_2 を使用するステップと、 G_{N1} および G_{N2} を使用するステップを備える。 g_1 は、 p に関連付けられる巡回群の生成元であり、 g_2 は、 q に関連付けられる巡回群の生成元である。 G_{N1} は、 g_1 に基づく定数であり、 G_{N2} は、 g_2 に基づく定数である。平文を暗号化するステップは、 s_1 および s_2 を使用するステップをさらに備える。 s_1 は、 p に基づく乱数であり、 s_2 は、 q に基づく乱数である。

【選択図】なし

【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、 $n = p \times q$ 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、 g_1 および g_2 を使用するステップを備え、前記 g_1 は、前記 p に関連付けられる巡回群の生成元であり、前記 g_2 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、 G_{N1} および G_{N2} を使用するステップをさらに備え、前記 G_{N1} は、前記 g_1 に基づく定数であり、前記 G_{N2} は、前記 g_2 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、 s_1 および s_2 を使用するステップをさらに備え、前記 s_1 は、前記 p に基づく乱数であり、前記 s_2 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 s_1 、前記 s_2 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、 $N = p \times q$ 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、 $n = p \times q$ 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、 g_1 および g_2 を使用することを備え、前記 g_1 は、前記 p に関連付けられる巡回群の生成元であり、前記 g_2 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】

10

20

30

40

50

前記対応する秘密鍵を使用する前記暗号化は、 $G N 1$ および $G N 2$ を使用することをさらに備え、前記 $G N 1$ は、前記 $g 1$ に基づく定数であり、前記 $G N 2$ は、前記 $g 2$ に基づく定数である、請求項 1 1 に記載のコンピュータ読取可能な媒体。

【請求項 1 3】

前記平文の前記暗号化は、 $s 1$ および $s 2$ を使用することをさらに備え、前記 $s 1$ は、前記 p に基づく乱数であり、前記 $s 2$ は、前記 q に基づく乱数である、請求項 1 0 に記載のコンピュータ読取可能な媒体。

【請求項 1 4】

【数 2】

前記平文の前記暗号化は、前記 $s 1$ 、前記 $s 2$ 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 1 3 に記載のコンピュータ読取可能な媒体。

10

【請求項 1 5】

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。

20

【請求項 1 6】

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、 $n = p \times q$ である、請求項 1 5 に記載の少なくとも 1 つのコンピュータ装置。

【請求項 1 7】

前記対応する秘密鍵を使用する前記暗号化は、 $g 1$ および $g 2$ を使用することを備え、前記 $g 1$ は、前記 p に関連付けられる巡回群の生成元であり、前記 $g 2$ 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 1 6 に記載の少なくとも 1 つのコンピュータ装置。

【請求項 1 8】

前記対応する秘密鍵を使用する前記暗号化は、 $G N 1$ および $G N 2$ を使用することをさらに備え、前記 $G N 1$ は、前記 $g 1$ に基づく定数であり、前記 $G N 2$ は、前記 $g 2$ に基づく定数である、請求項 1 7 に記載の少なくとも 1 つのコンピュータ装置。

30

【請求項 1 9】

前記平文の前記暗号化は、 $s 1$ および $s 2$ を使用することをさらに備え、前記 $s 1$ は、前記 p に基づく乱数であり、前記 $s 2$ は、前記 q に基づく乱数である、請求項 1 6 に記載の少なくとも 1 つのコンピュータ装置。

【請求項 2 0】

【数 3】

前記平文の前記暗号化は、前記 $s 1$ 、前記 $s 2$ 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 1 9 に記載の少なくとも 1 つのコンピュータ装置。

40

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

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】

50

【 0 0 0 2 】

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。

【 0 0 0 3 】

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。

【 0 0 0 4 】

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 】

【 0 0 0 5 】

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。

【 0 0 0 6 】

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 】

【 0 0 0 7 】

【 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 】

【 0 0 0 8 】

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。

【 0 0 0 9 】

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 1 0 0 は、公開鍵 1 0 2 の少なくとも一部と、対応する秘密鍵 1 0 4（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

10

20

30

40

50

うに実現される。高速暗号化 1 0 0 は、公開鍵 1 0 2 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。

【 0 0 1 0 】

高速暗号化 1 0 0 は、公開鍵などと秘密鍵など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: T L S)、プリティ・グッド・プライバシー (Pretty Good Privacy: P G P)、リベスト・シャミア・エーデルマン (Rivest, Shamir and Adleman: R S A)、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。

10

【 0 0 1 1 】

以下の図 2 に記載されているように、暗号文 C は、公開鍵 1 0 2 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 C 2 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 C 2 を復号化することができ、高速暗号化アルゴリズム 1 0 0 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。

20

【 0 0 1 2 】

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 A 2 0 0 (例えば、所有者) は、鍵生成 2 1 0 を用いて公開鍵 1 0 2 と秘密鍵 1 0 4 (または、復号鍵 1 0 4) とを生成する。鍵生成 1 2 0 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 1 0 2 は、暗号化されたメッセージを所有者 2 0 0 に送りたい任意のパーティ (例えば、パーティ B 2 5 0) に提供され得る。所有者 2 0 0 は、秘密鍵 1 0 4 を用いて、公開鍵 1 0 2 により暗号化されたメッセージを復号する。また、所有者 2 0 0 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 1 0 4 または秘密鍵 1 0 4 の少なくとも一部を用いる。

30

【 0 0 1 3 】

【数 1】

鍵生成 2 1 0 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 1 0 2 および秘密鍵 1 0 4）を生成する。実現例は、同等の長さ（例えば、2 5 6 ビット、5 1 2 ビット、1 0 2 4 ビット、2 0 4 8 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 1 0 2）を生成するために、鍵生成 2 1 0 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 $\mathbb{Z}_{n^2} = \{0, 1, \dots, (n^2 - 1)\}$ 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 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。

10

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。 $\mathbb{Z}_n = \{0, 1, \dots, (n-1)\}$ 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、EQ 1 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。

20

【0 0 1 4】

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 1 0 2 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 1 0 4）を生成するために、鍵生成 2 1 0 は、 $\lambda = \text{lcm}(p-1, q-1)$ を計算し、 lcm は最小公倍数である。また、鍵生成 2 1 0 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。

30

【0 0 1 5】

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。

【0 0 1 6】

例えば、 p および q は、5 1 2 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、1 0 2 4 ビットの長さの合成数であってもよい。 p および q が 1 0 2 4 ビットの長さの素数であれば、その結果として、 n は 2 0 4 8 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）。

40

【0 0 1 7】

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 q を用いて暗号化を行うことができる。高速暗号化 1 0 0 は、例えば、秘密鍵 1 0 4 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。

【0 0 1 8】

50

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、 $c = (g^m)(r^n) \bmod n^2$ である。g として $n+1$ が使用されると、暗号化式は、 $c = ((n+1)^m)(r^n) \bmod n^2$ になり、これは、 $(n+1)^m \bmod n^2$ の 2 項展開により、 $c = (1 + nm)(r^n) \bmod n^2$ (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。

10

【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「 $(r^n) \bmod n^2$ 」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】

20

なお、 $n^2 = p^2 q^2$ 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、 $p^2 q^2$ 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、 $(r^n) \bmod n^2 = (r^n) \bmod p^2 q^2$ は、乱数 r1 および r2 について $(r1)^n \bmod p^2$ および $(r2)^n \bmod q^2$ 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、 $y1 = (g1)^{s1} \bmod p^2$ 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。

30

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、 $y2 = (g2)^{s2} \bmod q^2$ 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、 $(y1)^n = [(g1)^{s1} \bmod p^2]^n = [(g1)^{s1}]^n \bmod p^2 = (g1^n)^{s1} \bmod p^2$ であり、 $(y2)^n = [(g2)^{s2} \bmod q^2]^n = [(g2)^{s2}]^n \bmod q^2 = (g2^n)^{s2} \bmod q^2$ である。参考までに、 $g1^n \bmod p^2$ は、GN1 として参照され得て、 $g2^n \bmod q^2 = GN2$ である。その結果、固定ベースの GN1 は、乱数 $s1 \bmod p^2$ の指数に累乗され (すなわち、 $GN1^{s1} \bmod p^2$)、固定ベースの GN2 は、乱数 $s2 \bmod q^2$ の指数に累乗される (すなわち、 $GN2^{s2} \bmod q^2$)。

40

【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、

50

2 5 6 ビットであってもよく、5 1 2 ビットであってもよく、1 0 2 4 ビットであってもよく、2 0 4 8 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。

【0 0 2 4】

【数 3】

$$p = 5, p^2 = 25$$

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

$$\Phi(p^2) = \mathbb{Z}^* p^2 \text{ のサイズ} = 20$$

p^2 の $g_1 = \{1:1, 2:20, 3:20, 4:10, 5:2, 6:5, 7:4, 8:20, 9:10, 10:2, 11:5, 12:20, 13:20, 14:10, 15:2, 16:5, 17:20, 18:4, 19:10, 20:2, 21:5, 22:20, 23:20, 24:2\}$ であり、最高次は 20 である。生成元 g_1 は、(2, 3, 8, 12, 13, 17, 22, または 23) であってもよい。

例えば、 $g_1 = 2$ である。

$$q = 7, q^2 = 49$$

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

$$\Phi(q^2) = \mathbb{Z}^* q^2 \text{ のサイズ} = 42$$

q^2 の $g_2 = \{1:1, 2:21, 3:42, 4:21, 5:42, 6:14, 7:2, 8:7, 9:21, 10:42, 11:21, 12:42, 13:14, 14:2, 15:7, 16:21, 17:42, 18:3, 19:6, 20:14, 21:2, 22:7, 23:21, 24:42, 25:21, 26:42, 27:14, 28:2, 29:7, 30:3, 31:6, 32:21, 33:42, 34:14, 35:2, 36:7, 37:21, 38:42, 39:21, 40:42, 41:14, 42:2, 43:7, 44:21, 45:42, 46:21, 47:42, 48:2\}$ であり、最高次は 42 である。生成元 g_2 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、 $g_2 = 3$ である。

$$n = pq = 35, n^2 = 35^2 = 1225$$

$$GN1 = g_1^n \bmod p^2 = 2^{35} \bmod 25 = 18$$

$$GN2 = g_2^n \bmod q^2 = 3^{35} \bmod 49 = 19$$

【0 0 2 5】

上記の定数値を事前計算した後、高速暗号化 1 0 0 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。

【0 0 2 6】

$EQ2$ は、 $c = (1 + nm)(r^n) \bmod n^2$ であり、「 $(r^n) \bmod n^2$ 」部分は、 $GN1^{s_1} \bmod p^2$ および $GN2^{s_2} \bmod q^2$ 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。

【0 0 2 7】

$D = (1 + nm) \bmod n^2$ 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。

【0 0 2 8】

実行されたように乱数要素 s_1 を $\Phi(p^2)$ から選択し、乱数要素 s_2 を $\Phi(q^2)$ か

10

20

30

40

50

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】

$E = GN1^{s1} \bmod p^2$ および $F = GN2^{s2} \bmod q^2$ 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 $H = (r^n) \bmod n^2$ 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。

10

【0031】

次いで、高速暗号化100は、 $c = DH \bmod n^2$ 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：

$$D = (1 + nm) \bmod n^2 = (1 + 35 \times 12) \bmod 35^2 = 421$$

$$s1 = 7 \text{ および } s2 = 9 \text{ (ランダムに選択される)}$$

$$E = GN1^{s1} \bmod p^2 = 18^7 \bmod 25 = 7$$

$$F = GN2^{s2} \bmod q^2 = 19^9 \bmod 49 = 48$$

20

Hは、以下の2つの式を用いて計算することができる

$$x \equiv 7 \bmod 25$$

$$x \equiv 48 \bmod 49$$

$$H = 832$$

$$C1 = DH \bmod n^2 = 421 \times 832 \bmod 1225 = 1147。$$

【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、 $m \in \mathbb{Z}_n$)、当該データは、各セグメント $\epsilon \in \mathbb{Z}_n$ 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。

30

【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を通して例えばパーティ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。

40

【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。

50

例えば、パーティ A 2 0 0 は、公開鍵 1 0 2 をパーティ B 2 5 0 に提供して、パーティ B は、メッセージ M 2 を暗号文 C 2 に暗号化してパーティ A に送る。M 2 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 2 6 0 は、 $EQ1c = (g^m)(r^n) \bmod n^2$ を用いて M 2 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 2 6 0 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。EQ 1 は、 $C2 = (g^m)(r^n) \bmod n^2 = (36^{12})(23^{35}) \bmod 1225 = 522$ になる。パーティ B は、C 2 をパーティ A に送る。なお、EQ 1 は、秘密鍵 1 0 4 (例えば、因数 p および q) または値 λ および μ もしくは μ を使用しない。

10

【0035】

パーティ A の復号化エンジン 2 3 0 は、C 1 (すなわち、秘密鍵 1 0 4 および公開鍵 1 0 2 を用いて高速暗号化 1 0 0 によって暗号化される) および C 2 (すなわち、公開鍵 1 0 2 だけを用いてパーティ B の暗号化エンジン 2 6 0 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。C 1 および C 2 が (例えば、別々に) いつ到達するかにかかわらず、C 1 および C 2 は、同一の復号化鍵または秘密鍵 1 0 4 (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 2 3 0 は、以下の値を抽出または計算する：

$$p = 5, q = 7, n = pq = 35, n^2 = 1225$$

$$g = n + 1 = 36$$

$$\lambda = lcm(p - 1, q - 1) = 12$$

$$\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n, \text{ ここで、} L(u) = (u - 1) / n \text{ である}$$

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

$$L(u) = (421 - 1) / 35 = 12$$

$$\mu = (12)^{-1} \bmod 35 = 3$$

$$\text{秘密鍵}(\lambda, \mu) = (12, 3)$$

復号化式は、 $m = L(c^\lambda \bmod n^2) \mu \bmod n$ である

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

20

30

【0037】

復号化エンジン 2 3 0 は、C 1 を復号化して平文 M 1 を取得し、C 2 を復号化して平文 M 2 を取得する。復号化エンジン 2 3 0 は、以下の値を計算して、C 1 (高速暗号化 1 0 0 によって生成された $C1 = 1147$) を復号化する：

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

$$k = (141 - 1) / 35 = 4$$

$$M1 = (k) \mu \bmod n = (4) 3 \bmod 35 = 12。$$

【0038】

復号化エンジン 2 3 0 は、以下の値を計算して、C 2 (暗号化エンジン 2 6 0 によって生成された $C2 = 522$) を復号化する：

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

$$k = (141 - 1) / 35 = 4$$

$$M2 = (k) \mu \bmod n = (4) 3 \bmod 35 = 12。$$

40

【0039】

C 1 が高速暗号化アルゴリズムを用いて暗号化され、C 2 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 2 3 0 が暗号文 C 1 および C 2 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 3 0 0 は、例えばブロック 3 1 0 を含

50

み、ブロック 3 1 0 において、高速暗号化 1 0 0 は、合成数 $n = p \times q$ (例えば、公開鍵 1 0 2) を用いてデータ (例えば、M 1) を暗号文 (例えば、C 1) 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 1 0 0 は、秘密鍵 1 0 4 の構成要素である p および q も個々に使用した。例えば、 g_1 および $G N_1$ は、 p を用いてまたは p に基づいて計算され、 g_2 および $G N_2$ は、 q を用いてまたは q に基づいて計算される。ブロック 3 2 0 において、暗号化されたデータ (例えば、C 1) は、(例えば、データベース 2 2 0 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 3 0 0 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 3 0 0 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、 $(e)(d) \equiv 1 \pmod{\phi(N)}$ 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 $m \pmod{p}$ および $m \pmod{q}$ を実行して、上記の EQ 2 の「 $(r^n) \pmod{n^2}$ 」部分の変換と同様の e 乗 $\pmod{N}$ 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 $\pmod{N}$ 合成体 N に累乗するオペレーションは、乱数 r_1 を p の n 番目の剰余から選択し、乱数 r_2 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、 r_1 および r_2 を組み合わせて、 $p q$ 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、 $(\sigma^e) \pmod{N} = (\sigma^e) \pmod{p q}$ は、乱数 r_1 および r_2 について $(r_1)^e \pmod{p}$ および $(r_2)^e \pmod{q}$ に変換されることができ、 $(r_1)(r_2) = \sigma$ 、 $r_1 \in \mathbb{Z}^*_p$ 、および $r_2 \in \mathbb{Z}^*_q$ である。オペレーションは、上記のように r_1 および r_2 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 4 0 0 は、装置 4 0 5 ~ 4 4 5 を含み、各々は、例えばネットワーク 4 6 0 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、モニター、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

10

20

30

40

50

てもよい。

【 0 0 5 2 】

コンピュータ装置 5 0 5 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。

【 0 0 5 3 】

コンピュータ装置 5 0 5 は、外部ストレージ 5 4 5 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 5 5 0 とに（例えば、I/Oインターフェース 5 2 5 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 5 0 5 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。

【 0 0 5 4 】

I/Oインターフェース 5 2 5 は、コンピュータ環境 5 0 0 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 5 0 0 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）、8 0 2 . 1 1 x、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 5 5 0 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）であってよい。

【 0 0 5 5 】

コンピュータ装置 5 0 5 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。

【 0 0 5 6 】

コンピュータ装置 5 0 5 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。

【 0 0 5 7 】

プロセッサ 5 1 0 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

10

20

30

40

50

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。

10

【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に必要な定数および/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。

20

【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。

30

【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とも実施可能であり、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。

40

【図 1】

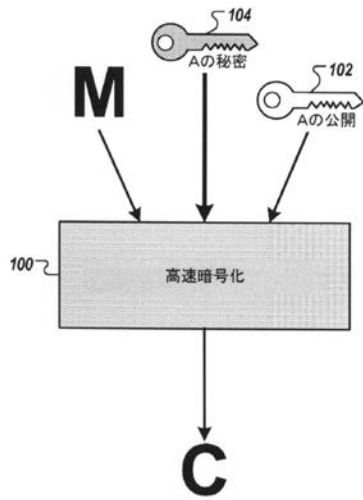


FIG. 1

【図 2】

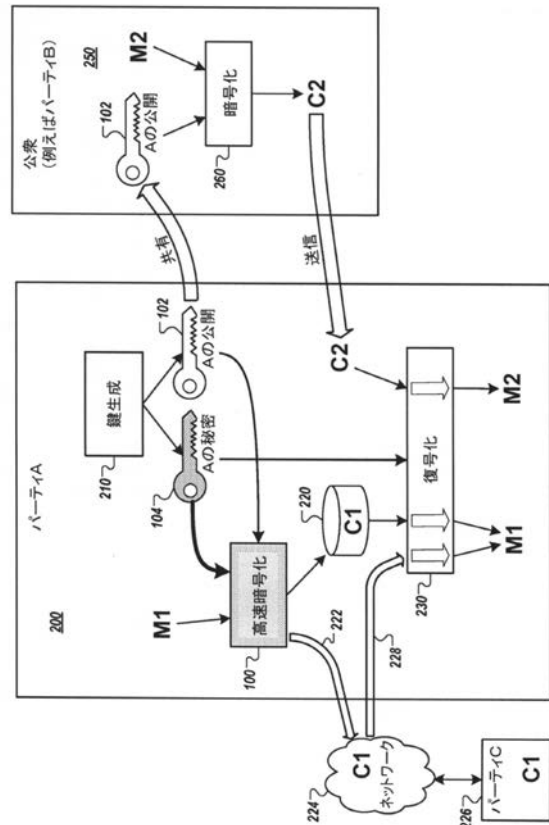


FIG. 2

【図 3】

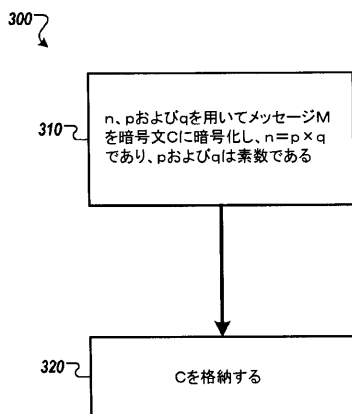


FIG. 3

【図 4】

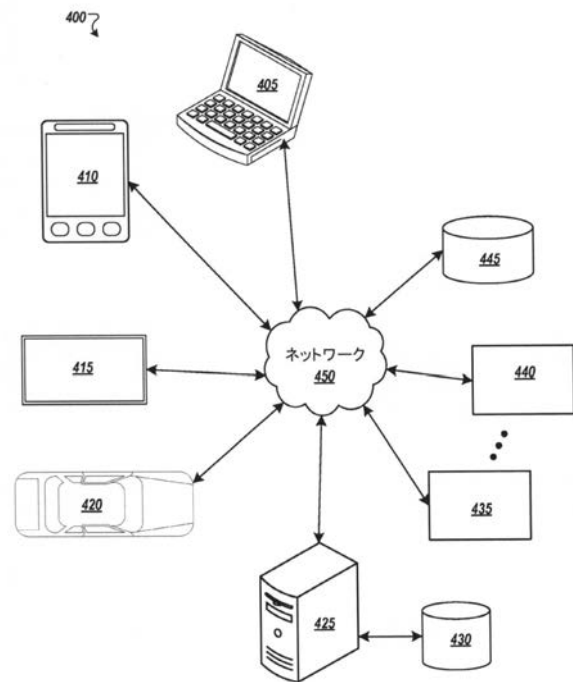


FIG. 4

【図 5】

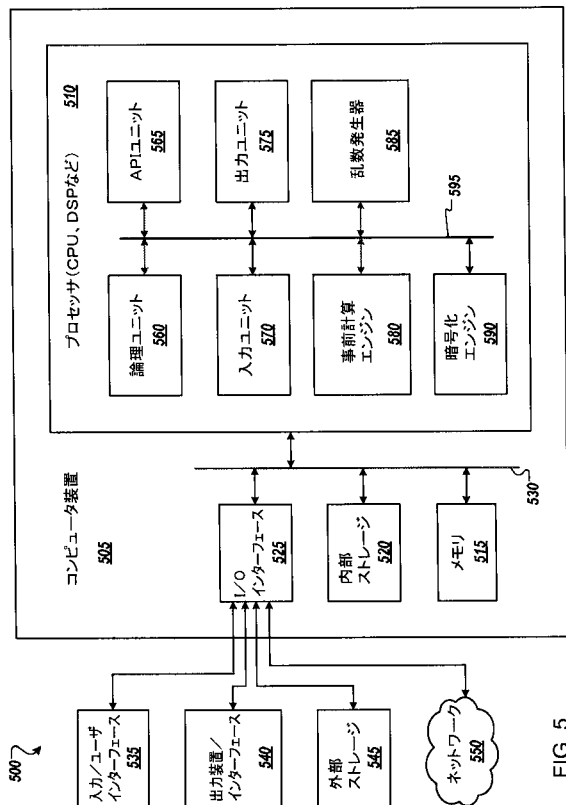


FIG. 5

【手続補正書】

【提出日】平成30年6月6日(2018.6.6)

【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、デジタル署名照合のための方法であって、
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 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
 $= p \times q$ である、請求項 1 に記載の方法。

【請求項 3】

デジタル署名照合のための方法をコンピュータに実行させるためのプログラムであって、
 、

前記方法は、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
するステップを含み、

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、前記照合結果を格納するステップをさらに含む、プログラム。

【請求項 4】

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

= $p \times q$ である、請求項 3 に記載のプログラム。

【請求項 5】

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、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
を生成する手段を含み、

前記生成する手段は、前記秘密鍵と、対応する公開鍵とを使用し、

前記プロセッサは、前記照合結果を格納する手段をさらに含む、少なくとも 1 つのコン
ピュータ装置。

【請求項 6】

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
= $p \times q$ である、請求項 5 に記載の少なくとも 1 つのコンピュータ装置。

フロントページの続き

(72)発明者 バテール, サーバー

アメリカ合衆国、9 4 0 4 3 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、1 6 0 0、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

【外国語明細書】
2018142013000001.pdf