(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2014-220668
(P2014-220668A)
(43)公開日　平成26年11月20日(2014.11.20)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
H04L	9/08	(2006.01)	H04L	9/00	601F	
			H04L	9/00	601C	

審査請求 未請求　請求項の数 9　ＯＬ　（全 22 頁）

(21)出願番号　特願2013-98964(P2013-98964)
(22)出願日　平成25年5月9日(2013.5.9)

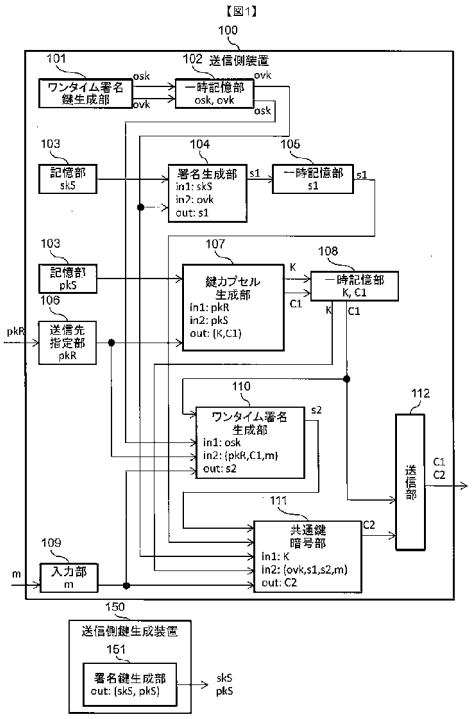
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(74)代理人　100098660
弁理士　戸田　裕二
(74)代理人　100091720
弁理士　岩崎　重美
(72)発明者　山本　暖
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所横浜研究所内

Ｆターム(参考)　5J104 AA01　AA09　EA06　EA16　EA19
JA31　KA05　KA21　LA03

(54)【発明の名称】送信側装置および受信側装置

(57)【要約】
【課題】メッセージ送受信時の通信速度の低下を抑えることでリアルタイム性の高い通信へ署名付き暗号化方式の適用を可能とするとともに、メッセージ送受信時に必要な計算を削減することで能力の十分でないプロセッサでも署名付き暗号化方式を実現すること。
【解決手段】送信側装置は、ワンタイム署名鍵生成部と、電子署名生成部と、タグベース鍵カプセル生成部と、から得た事前計算結果をそれぞれ一時的に記憶した後、送信するメッセージの内容が確定したならば、一時的に記憶した情報を利用して、ワンタイム署名生成部と共通鍵暗号部により署名と暗号文を生成し、一時結果の一部と合わせて受信側装置へ送信する。
【選択図】　図１

【図1】



【特許請求の範囲】
【請求項１】
メッセージから署名付き暗号文を生成して受信側装置へ送信する送信側装置であって、
送信者の、署名用秘密鍵および検証用公開鍵を記憶する記憶装置と、制御装置を具備し、
前記制御装置は、
ワンタイム署名用の鍵ペアを生成し、前記記憶装置に記憶するワンタイム署名鍵生成部と、
前記送信者の署名用秘密鍵を用いて、前記ワンタイム署名用の第一の鍵に対する第一の署名値を生成し、前記記憶装置に一時記憶する署名生成部と、
入力された前記メッセージの受信者の公開鍵および前記送信者の検証用公開鍵から共通鍵暗号用の鍵と該鍵の暗号化データを生成し、前記記憶装置に記憶する鍵カプセル生成部と、
前記ワンタイム署名用の第二の鍵、前記メッセージの受信者の公開鍵、前記共通鍵暗号用鍵の暗号化データ、および入力された送信対象メッセージから第二の署名値を生成するワンタイム署名生成部と、
前記共通鍵暗号用の鍵、前記ワンタイム署名用の第一の鍵、前記第一の署名値、前記第二の署名値、および前記送信対象メッセージから署名付き暗号文を生成する共通鍵暗号部と、
前記共通鍵暗号用の鍵の暗号化データおよび前記署名付き暗号文を前記受信側装置へ送信する送信部と、を含む、
ことを特徴とする送信側装置。
【請求項２】
前記ワンタイム署名用の第一の鍵は、ワンタイム署名を検証する際に必要なワンタイム署名用検証鍵であり、前記ワンタイム署名用の第二の鍵は、前記ワンタイム署名生成部で前記第二の署名値を生成する際に必要なワンタイム署名用秘密鍵である、
ことを特徴とする請求項１に記載の送信側装置。
【請求項３】
前記鍵カプセル生成部は、入力された前記メッセージの受信者の公開鍵およびタグとして前記記憶部から取得した前記送信者の検証用公開鍵から、タグ付き鍵カプセル生成アルゴリズムに基づいて、前記共通鍵暗号用の鍵と該鍵の暗号化データを生成し、前記記憶装置に記憶する、
ことを特徴とする請求項２に記載の送信側装置。
【請求項４】
前記鍵カプセル生成部は、前記ワンタイム署名用検証鍵と前記第一の署名値と前記送信者の検証用公開鍵とを結合したデータと、入力された前記メッセージの受信者の公開鍵から、共通鍵暗号用の鍵と該鍵の暗号化データを生成し、
前記ワンタイム署名生成部は、前記ワンタイム署名用秘密鍵、前記第一の署名値、入力された前記メッセージの受信者の公開鍵、前記共通鍵暗号用鍵の暗号化データおよび前記入力されたメッセージから、署名付き暗号文を生成し、
前記共通鍵暗号部は、前記共通鍵暗号用の鍵、前記第二の署名値および入力された前記メッセージから署名付き暗号文を生成し、
前記送信部は、前記ワンタイム署名用検証鍵、前記第一の署名値、前記共通鍵暗号用鍵の暗号化データおよび前記署名付き暗号文を前記受信側装置へ送信する、
ことを特徴とする請求項２に記載の送信側装置。
【請求項５】
送信側装置から受信した署名付き暗号文からメッセージを復号する受信側装置であって、
受信者の、復号用秘密鍵および暗号用公開鍵を記憶する記憶装置と、制御装置を具備し、

前記制御装置は、
前記送信側装置から共通鍵暗号用鍵の暗号化データおよび前記署名付き暗号文を受信する受信部と、
前記受信者の復号用秘密鍵、入力された送信者の検証用公開鍵および前記共通鍵暗号用鍵の暗号化データから、共通鍵暗号用鍵を復号する鍵カプセル復号部と、
前記共通鍵暗号用鍵を用いて、前記署名付き暗号文から、ワンタイム署名用の検証鍵、第一の署名値、第二の署名値および前記メッセージを復号する共通鍵復号部と、
前記ワンタイム署名用の検証鍵を検証対象メッセージとし、前記第一の署名値を検証対象署名値とし、前記送信者の検証用公開鍵を用いて署名検証を行う第一の署名検証部と、
前記受信者の暗号用公開鍵、前記受信部により受信した前記共通鍵暗号用鍵の暗号化データおよび前記共通鍵復号部により復号された前記メッセージを検証対象メッセージとし、前記第二の署名値を検証対象の署名値とし、前記ワンタイム署名の検証鍵を用いて署名検証を行う第二の署名検証部と、
前記鍵カプセル復号部により前記共通鍵暗号用鍵が復号され、前記第一の署名検証部および前記第二の署名検証部の検証結果がそれぞれ検証成功を示す場合に、前記共通鍵復号部により復号された前記メッセージを出力する出力部と、を含む、
ことを特徴とする受信側装置。
【請求項６】
前記出力部は、前記鍵カプセル復号部により前記共通鍵暗号用鍵の復号に失敗した場合、または前記第一の署名検証部の検証結果が検証失敗を示す場合、または前記第二の署名検証部の検証結果が検証失敗を示す場合、エラーコードを出力する、
ことを特徴とする請求項５に記載の受信側装置。
【請求項７】
前記鍵カプセル復号部は、前記受信者の復号用秘密鍵、タグとして入力された送信者の検証用公開鍵、および前記共通鍵暗号用鍵の暗号化データから、鍵カプセル復号アルゴリズムに基づいて、共通鍵暗号用鍵を復号する、
ことを特徴とする請求項６に記載の受信側装置。
【請求項８】
送信側装置から受信した署名付き暗号文からメッセージを復号する受信側装置であって、
受信者の、復号用秘密鍵および暗号用公開鍵を記憶する記憶装置と、制御装置を具備し、
前記制御装置は、
前記送信側装置から、ワンタイム署名用の検証鍵、第一の署名値、共通鍵暗号用鍵の暗号化データおよび署名付き暗号文を受信する受信部と、
前記受信者の復号用秘密鍵と、前記ワンタイム署名用の検証鍵と、前記第一の署名値と、入力された送信者の検証用公開鍵と、を用いて、前記共通鍵暗号用鍵の暗号化データから共通鍵暗号用鍵を復号する鍵カプセル復号部と、
前記ワンタイム署名用の検証鍵を検証対象メッセージとし、前記第一の署名値を検証対象署名値とし、前記送信者の検証用公開鍵を用いて署名検証を行う第一の署名検証部と、
前記鍵カプセル復号部により前記共通鍵暗号用鍵の復号に失敗した場合、または前記第一の署名検証部の処理結果が検証失敗を示す場合、エラーコードを出力部に出力し、そうでない場合、前記鍵カプセル復号部の処理により復号された前記共通鍵暗号用鍵を共通鍵復号部へ転送する第一判定部と、
前記第一判定部からの共通鍵暗号用鍵を用いて、復号対象の前記署名付き暗号文から第二の署名値とメッセージを復号する共通鍵復号部と、
前記第一の署名値、前記受信者の暗号用公開鍵、前記共通鍵暗号用鍵の暗号化データおよび前記共通鍵復号部により復号されたメッセージを検証対象メッセージとし、前記第二の署名値を検証対象の署名値とし、前記ワンタイム署名の検証鍵を用いて署名検証を行う第二の署名検証部と、

前記第二の署名検証部の処理結果が検証失敗を示す場合、エラーコードを出力部に出力し、そうでない場合、前記メッセージを出力部に出力する第二判定部と、
第一判定部または第二判定部の判定結果に基づいて、前記出力部に前記メッセージまたは前記エラーコードを出力する出力部と、を含む、
ことを特徴とする受信側装置。
【請求項９】
前記鍵カプセル復号部は、前記受信者の復号用秘密鍵と、タグとして入力された前記ワンタイム署名用の検証鍵と、タグとして入力された前記第一の署名値と、タグとして入力された送信者の検証用公開鍵と、を用いて、前記共通鍵暗号用鍵の暗号化データから共通鍵暗号用鍵を復号する、
ことを特徴とする請求項８に記載の受信側装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号および電子署名技術に関する。
【背景技術】
【０００２】
通信路の秘匿性を保証するため、すなわち通信路上を流れる情報を盗聴の脅威から守るための方法として、暗号技術の適用がよく知られている。また、通信路の真正性を保証するため、すなわち通信路上を流れる情報を改ざんや成りすましの脅威から守るための方法としては、電子署名技術の適用が知られている。さらに、秘匿性と真正性を同時に保証する技術として、暗号技術と電子署名技術を応用した署名付き暗号化（ｓｉｇｎｃｒｙｐｔｉｏｎ）技術が存在する。
【０００３】
署名付き暗号化技術の代表例として、Ｓｉｇｎ－ｔｈｅｎ－Ｅｎｃｒｙｐｔ方式とＥｎｃｒｙｐｔ－ｔｈｅｎ－Ｓｉｇｎ方式の２つがよく知られている。Ｓｉｇｎ－ｔｈｅｎ－Ｅｎｃｒｙｐｔ方式はメッセージに電子署名を付加した後、メッセージと署名値の組を暗号化する方式である。一方、Ｅｎｃｒｙｐｔ－ｔｈｅ－Ｓｉｇｎ方式はメッセージを公開鍵暗号で暗号化した後に、当該暗号文に対して電子署名を付加する方式である。
【０００４】
署名付き暗号化の安全性は、秘匿性と真正性の二つの側面から評価される。秘匿性に関しては、動的マルチユーザモデルにおいて内部者からの適応的選択暗号文攻撃に対して識別不可能性を有すること（ｄＭ－ＩＮＤ－ｉＣＣＡ：ＩＮＤｉｓｔｉｎｇｕｉｓｈａｂｉｌｉｔｙ ａｇａｉｎｓｔ ｉｎｓｉｄｅｒ Ｃｈｏｓｅｎ Ｃｉｐｈｅｒｔｅｘｔ Ａｔｔａｃｋ ｉｎ ｔｈｅｄｙｎａｍｉｃ Ｍｕｌｔｉ－ｕｓｅｒ ｍｏｄｅｌ と呼ばれる性質）が望まれる。また真正性に関しては、動的マルチユーザモデルにおいて内部者からの選択文書攻撃に対する強偽造不可能性を有すること（ｄＭ－ｓＵＦ－ｉＣＭＡ：ｓｔｒｏｎｇ ＵｎＦｏｒｇｅａｂｉｌｉｔｙ ａｇａｉｎｓｔｉｎｓｉｄｅｒ Ｃｈｏｓｅｎ Ｍｅｓｓａｇｅ Ａｔｔａｃｋ ｉｎ ｔｈｅ ｄｙｎａｍｉｃ Ｍｕｌｔｉ－ｕｓｅｒ ｍｏｄｅｌ と呼ばれる安全性基準）が望まれる。安全な署名付き暗号化方式は、これら２つの安全性を同時に満たすことが望ましいと考えられている。
【０００５】
前記のＳｉｇｎ－ｔｈｅｎ－Ｅｎｃｒｙｐｔ方式は、適応的選択暗号文攻撃に対する識別不可能性を有するが、選択文書攻撃に対する強偽造不可能性が保証されないことが分かっている。また、Ｅｎｃｒｙｐｔ－ｔｈｅｎ－Ｓｉｇｎ方式は、選択文書攻撃に対する強偽造不可能性を有する一方で、適応的選択暗号文攻撃に対する識別不可能性が保証されないことが知られている。
【０００６】
上記２つの安全性をともに備える署名付き暗号化方式として、非特許文献１に記載の方式が存在する。当該方式は、タグベースの鍵カプセル化メカニズム（通称ＴＢＫＥＭ）と

、電子署名方式、共通鍵暗号の３つの機能を組み合わせることで署名付き暗号化方式を実現したものである。構成要素であるＴＢＫＥＭ、電子署名、共通鍵暗号が、それぞれある安全性基準を満たす場合に、それらを組み合わせた署名付き暗号方式が前記の２つの安全性基準を満たすことが示されている。

【先行技術文献】

【非特許文献】

【０００７】

【非特許文献１】Ｄａｉｋｉ Ｃｈｉｂａ、Ｔａｋａｈｉｒｏ Ｍａｔｓｕｄａ、Ｊａｃｏｂ Ｃ.Ｎ. Ｓｃｈｕｌｄｔ、Ｋａｎｔａ Ｍａｔｓｕｕｒａ、″Ｅｆｆｉｃｉｅｎｔ Ｇｅｎｅｒｉｃ Ｃｏｎｓｔｒｕｃｔｉｏｎｓ ｏｆ Ｓｉｇｎｃｒｙｐｔｉｏｎ ｗｉｔｈ Ｉｎｓｉｄｅｒ Ｓｅｃｕｒｉｔｙ ｉｎ ｔｈｅ Ｍｕｌｔｉ−ｕｓｅｒ Ｓｅｔｔｉｎｇ、″ＡＣＮＳ ２０１１、ＬＮＣＳ ６７１５、ｐｐ.２２０−２３７、２０１１

【発明の概要】

【発明が解決しようとする課題】

【０００８】

秘匿性と真正性が同時に求められる分野は数多く存在する。例えば、証券会社のシステムから株式売買の発注を証券取引所のシステムへ送信する場合には、発注内容を取引所以外の他者に知られることを防ぐために秘匿性の確保が重要となると同時に、発注内容の改ざんや横取り（成りすまし）を防ぐために真正性の確保が求められる。またセンサネットワークやモバイルコンピューティングなどの分野においても、通信傍受を防ぐために秘匿性が要求され、かつメッセージの送信元を認証するために真正性が求められる。

【０００９】

上記の分野においては安全性の確保と同時に、処理性能に関する独自の制約が存在する。証券取引の場合、取引所へリクエストが集中する繁忙期には大量の注文を遅延なくリアルタイムに処理することが要求される。また後者の分野においては、個々のデバイスの計算能力がさほど高くなく、かつデバイスの省電力性が望まれるため、デバイスに要求される計算処理は単純なものであることが求められる。

【００１０】

非特許文献１に記載の方式は、前述した通り高い安全性を保証する一方で、内部で電子署名方式を利用しているため、通信のリアルタイム性および計算の複雑さに関する課題を内包している。

【００１１】

このような背景に鑑みて本発明がなされたのであり、本発明は、メッセージ送受信時の通信速度の低下を抑えることでリアルタイム性の高い通信へ署名付き暗号化方式の適用を可能とするとともに、メッセージ送受信時に必要な計算を削減することで能力の十分でないプロセッサでも署名付き暗号化方式を実現すること、を課題とする。

【課題を解決するための手段】

【００１２】

本発明の代表的な一例は、次の通りである。メッセージから署名付き暗号文を生成して受信側装置へ送信する送信側装置は、送信者の、署名用秘密鍵および検証用公開鍵を記憶する記憶装置と、制御装置を具備する。前記制御装置は、ワンタイム署名用の鍵ペアを生成し、前記記憶装置に記憶するワンタイム署名鍵生成部と、前記送信者の署名用秘密鍵を用いて、前記ワンタイム署名用の第一の鍵に対する第一の署名値を生成し、前記記憶装置に一時記憶する署名生成部と、入力された前記メッセージの受信者の公開鍵および前記送信者の検証用公開鍵から共通鍵暗号用の鍵と該鍵の暗号化データを生成し、前記記憶装置に記憶する鍵カプセル生成部と、前記ワンタイム署名用の第二の鍵、前記メッセージの受信者の公開鍵、前記共通鍵暗号用鍵の暗号化データ、および入力された送信対象メッセージから第二の署名値を生成するワンタイム署名生成部と、前記共通鍵暗号用の鍵、前記ワンタイム署名用の第一の鍵、前記第一の署名値、前記第二の署名値、および前記送信対象

メッセージから署名付き暗号文を生成する共通鍵暗号部と、前記共通鍵暗号用の鍵の暗号化データおよび前記署名付き暗号文を前記受信側装置へ送信する送信部と、を含む、ことを特徴とする。

【００１３】

また、送信側装置から受信した署名付き暗号文からメッセージを復号する受信側装置は、受信者の、復号用秘密鍵および暗号用公開鍵を記憶する記憶装置と、制御装置を具備する。前記制御装置は、前記送信側装置から共通鍵暗号用鍵の暗号化データおよび前記署名付き暗号文を受信する受信部と、前記受信者の暗号用秘密鍵、入力された送信者の検証用公開鍵および前記共通鍵暗号用鍵の暗号化データから、共通鍵暗号用鍵を復号する鍵カプセル復号部と、前記共通鍵暗号用鍵を用いて、前記署名付き暗号文から、ワンタイム署名用の検証鍵、第一の署名値、第二の署名値および前記メッセージを復号する共通鍵復号部と、前記ワンタイム署名用の検証鍵を検証対象メッセージとし、前記第一の署名値を検証対象署名値とし、前記送信者の検証用公開鍵を用いて署名検証を行う第一の署名検証部と、前記受信者の暗号用公開鍵、前記受信部により受信した前記共通鍵暗号用鍵の暗号化データおよび前記共通鍵復号部により復号された前記メッセージを検証対象メッセージとし、前記第二の署名値を検証対象の署名値とし、前記ワンタイム署名の検証鍵を用いて署名検証を行う第二の署名検証部と、前記鍵カプセル復号部により前記共通鍵暗号用鍵が復号され、前記第一の署名検証部および前記第二の署名検証部の検証結果がそれぞれ検証成功を示す場合に、前記共通鍵復号部により復号された前記メッセージを出力する出力部と、を含む、ことを特徴とする。

【発明の効果】

【００１４】

本発明によれば、高い安全性を備えるだけでなく、署名付き暗号化処理の大部分について事前計算が可能となる。これにより、リアルタイム性が要求されるシステムや能力が十分でないプロセッサに対しても、安全性の高い署名付き暗号化方式を適用できる。

【図面の簡単な説明】

【００１５】

【図１】実施形態１に係る送信側装置および送信側鍵生成装置の構成例を説明するための図である。

【図２】実施形態１に係る受信側装置および受信側鍵生成装置の構成例を説明するための図である。

【図３】実施形態１および２に係る各装置（クライアント装置、ゲートウェイ装置、データ管理装置）のハードウェア構成図である。

【図４】実施形態１および２に係る送信側装置および受信側装置が行う署名付き暗号文の送受信処理の全体の流れを示すシーケンス図である。

【図５】実施形態１に係る受信側装置における検証付き復号処理の流れを示すフローチャートである。

【図６】実施形態２に係る送信側装置および送信側鍵生成装置の構成例を説明するための図である。

【図７】実施形態２に係る受信側装置および受信側鍵生成装置の構成例を説明するための図である。

【図８】実施形態２に係る受信側装置における検証付き復号処理の流れを示すフローチャートである。

【発明を実施するための形態】

【００１６】

以下、図面を用いて本発明の実施の形態について説明する。なお、これにより本発明が限定されるものではない。

【実施例１】

【００１７】

図１は、本実施形態に係る送信側装置１００および送信側鍵生成装置１５０の構成例を

示す機能ブロック図である。

【００１８】

図１に示すように、送信側装置１００は、ワンタイム署名鍵生成部１０１、一時記憶部１０２、記憶部１０３、署名生成部１０４、一時記憶部１０５、送信先指定部１０６、鍵カプセル生成部１０７、一時記憶部１０８、入力部１０９、ワンタイム署名生成部１１０、共通鍵暗号部１１１、送信部１１２、とを含んで構成される。また、送信側鍵生成装置１５０は、署名鍵生成部１５１を含んで構成される。

【００１９】

署名生成部１０４と署名鍵生成部１５１、および後述する署名検証部２０６は、同じ電子署名アルゴリズムに基づく機能部である。すなわち、署名生成部１０４が実装する電子署名生成アルゴリズムと、署名鍵生成部１５１が実装する署名鍵生成アルゴリズムと、署名検証部２０６が実装する署名検証アルゴリズムと、は同じ電子署名方式に属するアルゴリズムである。したがって、署名鍵生成部１５１が出力した署名用鍵ペア（ｓｋＳ、ｐｋＳ）のうち、ｓｋＳは署名生成部１０４で署名を生成する際に必要な署名用秘密鍵として利用可能であり、ｐｋＳは署名検証部２０６で当該署名を検証する際に必要な署名用検証鍵として利用可能である。

【００２０】

同様に、ワンタイム署名生成部１１０とワンタイム署名鍵生成部１０１、および後述するワンタイム署名検証部２０７は、同じワンタイム署名方式に基づく機能部である。すなわち、ワンタイム署名生成部１１０が実装するワンタイム署名生成アルゴリズムと、ワンタイム署名鍵生成部１０１が実装するワンタイム署名鍵生成アルゴリズムと、ワンタイム署名検証部２０７が実装するワンタイム署名検証アルゴリズムと、は同じワンタイム署名方式に属するアルゴリズムである。したがって、ワンタイム署名鍵生成部１０１が出力したワンタイム署名用鍵ペア（ｏｓｋ、ｏｖｋ）のうち、ｏｓｋはワンタイム署名生成部１１０で署名を生成する際に必要な署名用秘密鍵として利用可能であり、ｏｖｋはワンタイム署名検証部２０７で当該署名を検証する際に必要な検証鍵として利用可能である。

【００２１】

また、鍵カプセル生成部１０７と後述する暗号鍵生成部２５１、および後述する鍵カプセル復号部２０４は、同一のタグ付き鍵カプセル化（ＴＢＫＥＭ）方式に基づく機能部である。すなわち、鍵カプセル生成部１０７が実装するタグ付き鍵カプセル生成アルゴリズムと、暗号鍵生成部２５１が実装する暗号鍵生成アルゴリズムと、鍵カプセル復号部２０４が実装する鍵カプセル復号アルゴリズムと、は同じＴＢＫＥＭ方式に属するアルゴリズムである。したがって、暗号鍵生成部２５１が出力した暗号用鍵ペア（ｓｋＲ、ｐｋＲ）のうち、ｐｋＲは鍵カプセル生成部１０７で鍵Ｋとそのカプセル化Ｃ１を生成する際に必要な暗号用公開鍵として利用可能であり、ｓｋＲは鍵カプセル復号部２０４でＣ１からＫを得る際に必要な復号用秘密鍵として利用可能である。

【００２２】

また、鍵カプセル生成部１０７の生成する鍵Ｋは、共通鍵暗号部１１１が暗号化処理を行う際の暗号鍵として利用可能である。

【００２３】

ワンタイム署名鍵生成部１０１は、ワンタイム署名鍵生成アルゴリズムを実装した機能部であり、ワンタイム署名用鍵ペア（ｏｓｋ、ｏｖｋ）を出力するものである。鍵ペア（ｏｓｋ、ｏｖｋ）は一時記憶部１０２への入力として利用される。

【００２４】

一時記憶部１０２は、ワンタイム署名の鍵ペア（ｏｓｋ、ｏｖｋ）を入力として、それらを一時的に、他の処理部によって消費されるまで記憶する。秘密鍵ｏｓｋはワンタイム署名生成部１１０への入力として後に利用される。公開鍵ｏｖｋは署名生成部１０４および共通鍵暗号部１１１への入力としてに後に利用される。ｏｓｋは送信者以外の者に知られることの無いよう、安全な記憶領域に格納されることが必要である。例えばＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）などといった製品を利用しても良い

。一時記憶部１０２には複数の鍵ペアを格納することが可能である。格納されるｏｓｋとｏｖｋには、一時記憶部１０２内で当該鍵ペアを一意に特定可能とする文字列、例えばシーケンス番号のような識別子を対応付けて管理する。以降、簡単のために当該文字列をラベルと呼ぶ。

【００２５】

記憶部１０３は、送信側鍵生成装置１５０によって生成された送信者の署名用秘密鍵ｓｋＳと検証用公開鍵ｐｋＳを記憶する。送信者の署名用秘密鍵ｓｋＳは、送信者以外の者に知られることの無いよう、安全な記憶領域に格納されることが必要である。例えばＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）などといった製品を利用しても良い。一方、送信者の検証用公開鍵ｐｋＳは、公開リポジトリや任意の通信手段を用いて、受信者を始め署名の検証を行う者へ広く公開されることが必要である。

【００２６】

署名生成部１０４は、電子署名生成アルゴリズムを実装した機能部である。署名鍵として送信者の署名用秘密鍵ｓｋＳを入力され、また署名対象メッセージとしてワンタイム署名の検証鍵ｏｖｋを入力され、処理の結果として署名値ｓ１を出力する。署名値ｓ１は一時記憶部１０５への入力として利用される。

【００２７】

一時記憶部１０５は、署名値ｓ１を入力として、それを一時的に、他の処理部によって消費されるまで記憶する。記憶された署名値ｓ１は共通鍵暗号部１１１への入力として後に利用される。一時記憶部１０５には複数の署名値を格納することが可能である。格納される署名値ｓ１には、一時記憶部１０５内で当該署名値を一意に特定可能なラベルが付与される。

【００２８】

送信先指定部１０６は、送信者がメッセージの送信先、すなわち受信者を決定した後に、当該受信者の暗号用公開鍵ｐｋＲを入力され、一時的に記憶する機能部である。暗号用公開鍵ｐｋＲは、鍵カプセル生成部１０７と、ワンタイム署名生成部１１０と、への入力として利用される。

【００２９】

鍵カプセル生成部１０７は、タグ付き鍵カプセル化アルゴリズムを実装した機能部である。カプセル化のための鍵として受信者の暗号用公開鍵ｐｋＲを入力され、またタグ（補助入力）として送信者の検証用公開鍵ｐｋＳを入力され、処理の結果として共通鍵暗号用の鍵Ｋと当該鍵をカプセル化（暗号化）した鍵カプセルＣ１を出力する。鍵Ｋと、鍵カプセルＣ１は一時記憶部１０８への入力として利用される。

【００３０】

一時記憶部１０８は、共通鍵暗号用の鍵Ｋと当該鍵をカプセル化（暗号化）した鍵カプセルＣ１を入力として、それらを一時的に、他の処理部によって消費されるまで記憶する。鍵カプセルＣ１はワンタイム署名生成部１１０および送信部１１２への入力として後に利用される。鍵Ｋは共通鍵暗号部１１１への入力として後に利用される。鍵Ｋは送信者以外の者に知られることの無いよう、安全な記憶領域に格納されることが必要である。例えばＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）などといった製品を利用しても良い。一時記憶部１０８には複数の鍵および鍵カプセルを格納することが可能である。格納される鍵と鍵カプセルのペア（Ｋ、　Ｃ１）には、一時記憶部１０８内で当該ペアを一意に特定可能なラベルが付与される。

【００３１】

入力部１０９は、送信者が送信対象メッセージを決定した後に、当該メッセージｍを入力される機能部である。メッセージｍは、ワンタイム署名生成部１１０と、共通鍵暗号部１１１への入力として利用される。

【００３２】

ワンタイム署名生成部１１０は、署名鍵としてワンタイム署名の署名用秘密鍵ｏｓｋを入力され、また署名対象メッセージとして受信者の暗号用公開鍵ｐｋＲと、鍵カプセルＣ

１と、メッセージｍと、を入力され、処理の結果として署名値ｓ２を出力する。署名値ｓ２は共通鍵暗号部１１１の入力として利用される。

【００３３】

共通鍵暗号部１１１は、暗号鍵として鍵Ｋを入力され、また暗号化対象メッセージとしてワンタイム署名の検証鍵ｏｖｋと、署名値ｓ１と、署名値ｓ２と、メッセージｍと、を入力され、処理の結果として暗号文Ｃ２を出力する。暗号文Ｃ２は送信部１１２の入力として利用される。

【００３４】

送信部１１２は、鍵カプセルＣ１と、暗号文Ｃ２と、が入力された後、これらを受信側装置２００へ送信する。通信にはＴＣＰ／ＩＰやＨＴＴＰ等の汎用的なプロトコルを利用可能である。

【００３５】

図２は、本実施形態に係る受信側装置２００および受信側鍵生成装置２５０の構成例を示す機能ブロック図である。

【００３６】

図２に示すように、送信側装置２００は、送信元指定部２０１、受信部２０２、記憶部２０３、鍵カプセル復号部２０４、共通鍵復号部２０５、署名検証部２０６、ワンタイム署名検証部２０７、判定部２０８、出力部２０９とを含んで構成される。また、受信側鍵生成装置２５０は、暗号鍵生成部２５１を含んで構成される。

【００３７】

前述した通り、署名検証部２０６と先述の署名生成部１０４および署名鍵生成部１５１は、同じ電子署名アルゴリズムに基づく機能部である。また、ワンタイム署名検証部２０７と先述のワンタイム署名生成部１１０およびワンタイム署名鍵生成部１０１は、同じワンタイム署名方式に基づく機能部である。また、暗号鍵生成部２５１および鍵カプセル復号部２０４と、先述の鍵カプセル生成部１０７は、同一のタグ付き鍵カプセル化（ＴＢＫＥＭ）方式に基づく機能部である。

【００３８】

送信元指定部２０１は、受信者がメッセージの送信元、すなわち送信者（の候補）を把握した後に、当該送信者の検証用公開鍵ｐｋＳを入力され、一時的に記憶する機能部である。検証用公開鍵ｐｋＳは、鍵カプセル復号部２０４と、署名検証部２０６と、への入力として利用される。

【００３９】

受信部２０２は、鍵カプセルＣ１と、暗号文Ｃ２と、を送信側装置１００から受信した後、これらを必要に応じて各機能部へ転送する。受信にはＴＣＰ／ＩＰやＨＴＴＰ等の汎用的なプロトコルを利用可能である。

【００４０】

記憶部２０３は、受信側鍵生成装置２５０によって生成された受信者の復号用秘密鍵ｓｋＲと暗号用公開鍵ｐｋＲを記憶する。受信者の復号用秘密鍵ｓｋＲは、受信者以外の者に知られることの無いよう、安全な記憶領域に格納されることが必要である。例えばＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）などといった製品を利用しても良い。一方、受信者の暗号用公開鍵ｐｋＲは、公開リポジトリや任意の通信手段を用いて、送信者を始め当該受信者へのメッセージ送信を行う者へ広く公開されることが必要である。

【００４１】

鍵カプセル復号部２０４は、タグ付き鍵カプセル復号アルゴリズムを実装した機能部である。カプセル復号のための鍵として受信者の暗号用秘密鍵ｓｋＲを入力され、またタグ（補助入力）として送信者の検証用公開鍵ｐｋＳを入力され、また復号対象の鍵カプセルＣ１を入力され、処理の結果として共通鍵暗号用の鍵ＫまたはエラーコードＥＲＲを出力する。鍵ＫまたはエラーコードＥＲＲは共通鍵復号部２０５および判定部２０８への入力として利用される。

【００４２】
共通鍵復号部２０５は、鍵Ｋと暗号文Ｃ２を入力され、処理の結果として検証鍵ｏｖｋと、署名値ｓ１と、署名値ｓ２と、メッセージｍと、を出力する。検証鍵ｏｖｋは署名検証部２０６およびワンタイム署名検証部２０７への入力として利用される。署名値ｓ１は署名検証部２０６への入力として利用される。メッセージｍおよび署名値ｓ２はワンタイム署名検証部２０７への入力として利用される。
【００４３】
署名検証部２０６は、電子署名検証アルゴリズムを実装した機能部である。検証鍵として送信者の検証用公開鍵ｐｋＳを入力され、検証対象メッセージとしてワンタイム署名の検証鍵ｏｖｋを入力され、署名値としてｓ１を入力され、処理の結果として検証結果ｖ１（検証成功または検証失敗の二値）を出力する。検証結果ｖ１は判定部２０８への入力として利用される。
【００４４】
ワンタイム署名検証部２０７は、検証鍵としてワンタイム署名の検証鍵ｏｖｋを入力され、また検証対象メッセージとして受信者の暗号用公開鍵ｐｋＲと、鍵カプセルＣ１と、メッセージｍと、を入力され、処理の結果として検証結果ｖ２（検証成功または検証失敗の二値）を出力する。検証結果ｖ２は判定部２０８の入力として利用される。
【００４５】
判定部２０８は、鍵カプセル復号部２０４の処理結果がエラーコードＥＲＲであるか、または署名検証部２０６の処理結果ｖ１が検証失敗であるか、またはワンタイム署名検証部２０７の処理結果ｖ２が検証失敗であるか、いずれかの場合には、出力部２１０を介してエラーコードＥＲＲを受信者へ提示することで、受信した暗号文（Ｃ１、Ｃ２）に問題があったことを示す。そうでない場合、共通鍵復号部２０５によって復号されたメッセージｍを、出力部２０９を介して受信者へ提示する。この場合、受信者が受け取ったメッセージｍは確かに送信元指定部２０１によって指定された送信者から送られたものであることが保証される。
【００４６】
出力部２１０は、判定部２０８の判定結果に基づいて受信側装置２００の利用者（受信者）へメッセージｍまたはエラーコードＥＲＲを提示する。
【００４７】
図３は、本実施形態に係る各装置（送信側装置１００、送信側鍵生成装置１５０、受信側装置２００、受信側鍵生成装置２５０）のハードウェア構成図である。
【００４８】
図３に示すように、本実施形態に係る各装置は、一般的なコンピュータ３００により実現される。
【００４９】
コンピュータ３００は、ＣＰＵ３０１と、メモリ３０２と、ハードディスク等の外部記憶装置３０３と、通信ネットワークに接続するためのＮＩＣ（Ｎｅｔｗｏｒｋ　ＩｎｔｅｒｆａｃｅＣａｒｄ）等の送受信装置３０４と、モニタ等の出力装置３０５と、キーボードやマウス等の入力装置３０６と、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の可搬性を有する記憶媒体３０８から情報を読み取る読取装置３０７とを含んで構成される。
【００５０】
そして、各装置の記憶部内の記憶領域は、ＣＰＵ３０１がメモリ３０２または外部記憶装置３０３を利用することにより実現可能となる。また、各制御部は、外部記憶装置３０３に記憶されている所定のプログラムをメモリ３０２にロードすることによりＣＰＵ３０１で実現可能となる。この所定のプログラムは、読取装置３０７を介して記憶媒体３０８から取得してもよいし、送受信装置３０４を介してネットワークから外部記憶装置３０３にダウンロードされ、メモリ３０２にロードされてＣＰＵ３０１により実行されるようにしてもよい。また、読取装置３０７を介して記憶媒体３０８から、あるいは、送受信装置３０４を介してネットワークから、メモリ３０２に直接ロードされ、ＣＰＵ３０１により

実行されるようにしてもよい。

【００５１】

次に、図４を参照して、本実施形態に係る各装置（送信側装置１００、送信側鍵生成装置１５０、受信側装置２００、受信側鍵生成装置２５０）による署名付き暗号文の送受信処理について説明する。

【００５２】

まず、送信側装置１００は、以降の署名付き暗号化処理で使用するためのワンタイム署名鍵を生成する（ステップ４０１）。具体的には、送信側装置１００のワンタイム署名鍵生成部１０１が、ワンタイム署名鍵生成アルゴリズムに基づいてワンタイム署名用の鍵ペア（ｏｓｋ、　ｏｖｋ）を生成し、一時記憶部１０２に保存する。この際、ｏｓｋおよびｏｖｋには当該鍵ペアを一時記憶部１０２内で一意に特定可能とするラベルが付与される。当該ワンタイム署名鍵生成処理には、送信者の鍵ペア（ｓｋＳ、　ｐｋＳ）、受信者の公開鍵ｐｋＲ、メッセージｍのいずれも必要とされないため、他の処理とは独立に計算することが可能である。この点を活用し、送信側装置１００の起動時や起動中のアイドル時間に当該ワンタイム署名鍵生成処理を複数回計算し、結果（ワンタイム署名用鍵ペア）を一時記憶部１０２へ保存しておくことで、ステップ４０２以降にかかる処理時間を短縮することが可能である。

【００５３】

次に、送信側鍵生成装置１５０が、署名鍵生成部１５１を用いて送信者の署名用鍵ペア（ｓｋＳ、　ｐｋＳ）を生成する（ステップ４０２）。生成された鍵ペア（ｓｋＳ、　ｐｋＳ）は記憶部１０３に保存される。

【００５４】

次に、送信側装置１００が、ワンタイム署名の検証鍵ｏｖｋに署名値ｓ１を付与する（ステップ４０３）。具体的には、送信側装置１００の署名生成部１０４が、記憶部１０３に格納された送信者の秘密鍵ｓｋＳを署名鍵として入力されるとともに、一時記憶部１０２に保存されたワンタイム署名用の検証鍵ｏｖｋを署名対象メッセージとして入力されることで、署名生成アルゴリズムに基づいて署名値ｓ１を出力する。出力された署名値ｓ１は、入力された検証鍵ｏｖｋのラベルと同じ識別子を付与した状態で、一時記憶部１０５に格納される。当該署名生成処理には、受信者の公開鍵ｐｋＲ、メッセージｍのいずれも必要とされないため、ステップ４０４以降の処理とは独立に事前計算することが可能である。この点を活用し、送信側鍵生成装置１５０によって署名用鍵ペア（ｓｋＳ、　ｐｋＳ）が生成された後、装置起動中のアイドル時間に、一時記憶部１０１に格納されたワンタイム署名用の鍵ペア群に署名付与を実施し、結果（ワンタイム署名用鍵ペアに付与した署名値）を一時記憶部１０５へ保存しておくことで、ステップ４０４以降にかかる処理時間を短縮することが可能である。

【００５５】

次に、送信側装置１００は、送信者からの入力に従い、メッセージの送信先を決定する（ステップ４０４）。具体的には、送信者は、受信者の公開鍵ｐｋＲを公開リポジトリや任意の通信手段を用いて取得し、送信側装置１００の送信先指定部１０６へ入力する。

【００５６】

次に、送信側装置１００が、鍵カプセルを生成する（ステップ４０５）。具体的には、送信側装置１００の鍵カプセル生成部１０７が、送信先指定部１０６の取得した送信先（受信者）の公開鍵ｐｋＲを暗号鍵として入力されるとともに、記憶部１０３に格納された送信者の公開鍵ｐｋＳをタグとして入力されることで、タグ付き鍵カプセル生成アルゴリズムに基づいて、共通鍵暗号用の鍵Ｋと、当該鍵をカプセル化した鍵カプセルＣ１と、を出力する。出力された（Ｋ、　Ｃ１）は一時記憶部１０８へ保存される。この際、ＫおよびＣ１には当該ペアを一意に特定可能なラベルを付与して格納する。

【００５７】

次に、送信側装置１００は、送信者からの入力に従い、送信すべきメッセージを決定する（ステップ４０６）。具体的には、送信者は、送信側装置１００の入力部１０９に対し

て送信すべきメッセージｍを入力する。
【００５８】
次に、送信側装置１００は、ワンタイム署名を生成する（ステップ４０７）。具体的には、送信側装置１００のワンタイム署名生成部１１０が、一時記憶部１０２に保存されたワンタイム署名用の秘密鍵ｏｓｋを署名鍵として入力されるとともに、送信先指定部１０６によって取得された受信者の公開鍵ｐｋＲと、一時記憶部１０８に保存された鍵カプセルＣ１と、入力部１０７によって取得されたメッセージｍと、を送信対象の文書として入力されることで、ワンタイム署名生成アルゴリズムを実行し、署名値ｓ２を出力する。
【００５９】
次に、送信側装置１００は、暗号文を生成する（ステップ４０８）。具体的には、送信側装置１００の共通鍵暗号部１１１が、一時記憶部１０８に格納された鍵のうち、ステップ４０７で利用した鍵カプセルＣ１と同じラベルを持つ鍵Ｋを選択し、暗号鍵として利用する。また、一時記憶部１０２に保存された検証鍵のうち、ステップ４０７で利用した秘密鍵ｏｓｋと同じラベルを持つ検証鍵ｏｖｋと、一時記憶部１０５に保存された署名値ｓ１と、ワンタイム署名生成部１１０が生成した署名値ｓ２と、入力部１０９が取得したメッセージｍと、を暗号化対象メッセージとして入力されることで、共通鍵暗号アルゴリズムを実行し、暗号文Ｃ２を出力する。
【００６０】
最後に、送信側装置１００の送信部１１２が、ステップ４０７で利用した鍵カプセルＣ１と、共通鍵暗号部１１１が出力した暗号文Ｃ２と、から構成される署名付き暗号文（Ｃ１、Ｃ２）を、ネットワークを介して受信側装置２００へ送信する（ステップ４０９）。メッセージ送信後には、ステップ４０１からステップ４０９の間に利用された鍵ペア（ｏｓｋ、ｏｖｋ）、　署名値ｓ１、　鍵と鍵カプセル（Ｋ、　Ｃ１）は、それぞれ一時記憶部１０２、　１０５、１０８から消去される。
【００６１】
以上が送信側装置１００によって実行される署名付き暗号化処理の具体的な流れである。
【００６２】
次に受信側装置２００によって実行される検証付き復号処理の具体的な流れについて説明する。受信側装置２００は、送信側装置１００によって送信された署名付き暗号文（Ｃ１、　Ｃ２）を受信すると、まず、当該署名付き暗号文の送信者（送信側装置１００の利用者）を特定し、当該送信者の公開鍵ｐｋＳを受信側装置２００の送信元指定部２０１へ入力する（ステップ４１０）。当該公開鍵ｐｋＳは署名付き暗号文とともに送信者から送信されることもあれば、公開リポジトリなどから取得されることも可能である。
【００６３】
次に、受信側装置２００は、特定した送信者公開鍵ｐｋＳを元に、受信した署名付き暗号文（Ｃ１、　Ｃ２）の検証付き復号処理を実行する（ステップ４１１）。
【００６４】
ここで図５を用いて、当該検証付き復号処理の具体的な流れについて説明する。
【００６５】
まず、受信側装置２００の鍵カプセル復号部２０４が、記憶部２０３に格納された受信者の秘密鍵ｓｋＲを復号鍵として入力されるとともに、送信元指定部２０１が取得したｐｋＳをタグとして入力され、また受信部２０２が受信したＣ１を復号対象の鍵カプセルとして入力される。鍵カプセル復号部２０４は鍵カプセル復号アルゴリズムを実行し、復号に成功した場合は鍵Ｋを出力し、失敗した場合は復号エラーを示すコードＥＲＲを出力する（ステップ５０１）。
【００６６】
次に、受信側装置２００の共通鍵復号部２０５が、鍵カプセル復号部２０４が出力した鍵Ｋを復号用の鍵として入力されるとともに、受信部２０２が受信した暗号文Ｃ２を復号対象の暗号文として入力される。共通鍵復号部２０５は共通鍵復号アルゴリズムを実行し

、復号に成功した場合は復号結果である（ｏｖｋ、　ｓ１、　ｓ２、　ｍ）を出力し、失敗した場合はエラーを示すコードＥＲＲを出力する（ステップ５０２）。

【００６７】

次に、受信側装置２００の署名検証部２０６は、送信元指定部２０１に格納された送信者の公開鍵ｐｋＳを検証鍵として入力されるとともに、共通鍵復号部２０５によって出力されたｏｖｋを検証対象メッセージとして入力され、また共通鍵復号部２０５によって出力された署名値ｓ１を検証対象の署名値として入力される。署名検証部２０６は署名検証アルゴリズムを実行し、検証に成功した場合は１を、失敗した場合は０を出力する（ステップ５０３）。

【００６８】

次に、受信側装置２００のワンタイム署名検証部２０７が、受信部２０２が受信したｏｖｋを検証鍵として入力されるとともに、記憶部２０３に格納された受信者の公開鍵ｐｋＲと、受信部２０２によって受信された鍵カプセルＣ１と、共通鍵復号部２０５の出力したメッセージｍと、を検証対象の文書として入力され、また共通鍵復号部２０５の出力した署名値ｓ２を検証対象の署名値として入力される。ワンタイム署名検証部２０７は、ワンタイム署名の検証アルゴリズムを実行し、検証に成功した場合は１を、失敗した場合は０を出力する（ステップ５０４）。

【００６９】

次に、受信側装置２００の判定部２０８が、鍵カプセル復号部２０４の出力と、署名検証部２０６の出力と、ワンタイム署名検証部２０７の出力と、に基づいて処理の継続可否を判定する（ステップ５０５）。具体的には、鍵カプセル復号部２０４が鍵Ｋの出力に成功し、かつ署名検証部２０６による検証結果が１（受理）で、かつワンタイム署名検証部２０７による検証結果が１（受理）であった場合のみ、メッセージｍを出力部２１０を介して受信者へ出力し（ステップ５０６）、そうでない場合には検証エラーを示すコードＥＲＲを出力部２１０を介して受信者へ出力する（ステップ５０７）。

【００７０】

以上が受信側装置２００によって実行される検証付き復号処理の具体的な流れである。

【００７１】

以上説明したように、本実施形態に係る送信側装置１００によれば、ワンタイム署名鍵生成処理を他の処理とは独立にいつでも事前計算することが可能となる。また、送信者の署名用鍵ペア（ｓｋＳ、　ｐｋＳ）が決定した後であれば、メッセージの送信先（受信者）や送信すべきメッセージの内容が決まる前の段階であっても、署名生成処理を事前計算することが可能となる。また、送信先受信者の公開鍵ｐｋＲが決定した後であれば、送信すべきメッセージの内容が決まる前の段階でも、鍵カプセル生成処理を事前計算することが可能となる。計算コストの高い署名生成処理や鍵カプセル生成処理を事前計算しておくことで、送信すべきメッセージｍが決定された後の処理を共通鍵暗号およびワンタイム署名といった計算コストの低い処理のみで実現できるため、メッセージ決定から送信までに要する時間を短縮することが可能となる。

【実施例２】

【００７２】

図６は、本実施形態に係る送信側装置６００および送信側鍵生成装置６５０の構成例を示す機能ブロック図である。

【００７３】

図６に示すように、送信側装置６００は、ワンタイム署名鍵生成部６０１、一時記憶部６０２、記憶部６０３、署名生成部６０４、一時記憶部６０５、送信先指定部６０６、鍵カプセル生成部６０７、一時記憶部６０８、入力部６０９、ワンタイム署名生成部６１０、共通鍵暗号部６１１、送信部６１２、とを含んで構成される。また、送信側鍵生成装置６５０は、署名鍵生成部６５１を含んで構成される。

【００７４】

署名生成部６０４と署名鍵生成部６５１、および後述する署名検証部７０５は、同じ電

子署名アルゴリズムに基づく機能部である。すなわち、署名生成部６０４が実装する電子署名生成アルゴリズムと、署名鍵生成部６５１が実装する署名鍵生成アルゴリズムと、署名検証部７０５が実装する署名検証アルゴリズムと、は同じ電子署名方式に属するアルゴリズムである。したがって、署名鍵生成部６５１が出力した署名用鍵ペア（ｓｋＳ、ｐｋＳ）のうち、ｓｋＳは署名生成部６０４で署名を生成する際に必要な署名用秘密鍵として利用可能であり、ｐｋＳは署名検証部７０５で当該署名を検証する際に必要な署名用検証鍵として利用可能である。

【００７５】

同様に、ワンタイム署名生成部６１０とワンタイム署名鍵生成部６０１、および後述するワンタイム署名検証部７０８は、同じワンタイム署名方式に基づく機能部である。すなわち、ワンタイム署名生成部６１０が実装するワンタイム署名生成アルゴリズムと、ワンタイム署名鍵生成部６０１が実装するワンタイム署名鍵生成アルゴリズムと、ワンタイム署名検証部７０８が実装するワンタイム署名検証アルゴリズムと、は同じワンタイム署名方式に属するアルゴリズムである。したがって、ワンタイム署名鍵生成部６０１が出力したワンタイム署名用鍵ペア（ｏｓｋ、ｏｖｋ）のうち、ｏｓｋはワンタイム署名生成部６１０で署名を生成する際に必要な署名用秘密鍵として利用可能であり、ｏｖｋはワンタイム署名検証部７０８で当該署名を検証する際に必要な検証鍵として利用可能である。

【００７６】

また、鍵カプセル生成部６０７と後述する暗号鍵生成部７５１、および後述する鍵カプセル復号部７０４は、同一のタグ付き鍵カプセル化（ＴＢＫＥＭ）方式に基づく機能部である。すなわち、鍵カプセル生成部６０７が実装するタグ付き鍵カプセル生成アルゴリズムと、暗号鍵生成部７５１が実装する暗号鍵生成アルゴリズムと、鍵カプセル復号部７０４が実装する鍵カプセル復号アルゴリズムと、は同じＴＢＫＥＭ方式に属するアルゴリズムである。したがって、暗号鍵生成部７５１が出力した暗号用鍵ペア（ｓｋＲ、ｐｋＲ）のうち、ｐｋＲは鍵カプセル生成部６０７で鍵Ｋとそのカプセル化Ｃ１を生成する際に必要な暗号用公開鍵として利用可能であり、ｓｋＲは鍵カプセル復号部７０４でＣ１からＫを得る際に必要な復号用秘密鍵として利用可能である。

【００７７】

また、鍵カプセル生成部６０７の生成する鍵Ｋは、共通鍵暗号部６１１が暗号化処理を行う際の暗号鍵として利用可能である。

【００７８】

以下、ワンタイム署名鍵生成部６０１、記憶部６０３、署名生成部６０４、送信先指定部６０６、一時記憶部６０８、入力部６０９、送信側鍵生成装置６５０、署名鍵生成部６５１、については、それぞれ実施形態１のワンタイム署名鍵生成部１０１、記憶部１０３、署名生成部１０４、送信先指定部１０６、一時記憶部１０８、入力部１０９、送信側鍵生成装置１５０、署名鍵生成部１５１、と同様の構成となるため、詳細な説明は省略する。

【００７９】

一時記憶部６０２は、ワンタイム署名の鍵ペア（ｏｓｋ、ｏｖｋ）を入力として、それらを一時的に、他の処理部によって消費されるまで記憶する。秘密鍵ｏｓｋはワンタイム署名生成部６１０への入力として後に利用される。検証鍵ｏｖｋは署名生成部６０４と、鍵カプセル生成部６０７と、送信部６１２と、への入力としてに後に利用される。ｏｓｋは送信者以外の者に知られることの無いよう、安全な記憶領域に格納されることが必要である。例えばＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）などといった製品を利用しても良い。一時記憶部６０２には複数の鍵ペアを格納することが可能である。格納されるｏｓｋとｏｖｋには、一時記憶部６０２内で当該鍵ペアを一意に特定可能とする文字列、例えばシーケンス番号のような識別子を対応付けて管理する。以降、簡単のために当該文字列を単にラベルと呼ぶ。

【００８０】

一時記憶部６０５は、署名値ｓ１を入力として、それを一時的に、他の処理部によって

消費されるまで記憶する。記憶された署名値ｓ１は鍵カプセル生成部６０７と、ワンタイム署名生成部６１０と、送信部６１２と、への入力として後に利用される。一時記憶部６０５には複数の署名値を格納することが可能である。格納される署名値ｓ１には、一時記憶部６０５内で当該署名値を一意に特定可能なラベルが付与される。

【００８１】

鍵カプセル生成部６０７は、タグ付き鍵カプセル化アルゴリズムを実装した機能部である。カプセル化のための鍵として受信者の暗号用公開鍵ｐｋＲを入力され、またタグ（補助入力）として、ワンタイム署名の検証鍵ｏｖｋと、署名値ｓ１と、送信者の検証用公開鍵ｐｋＳと、を結合したものを入力され、処理の結果として共通鍵暗号用の鍵Ｋと当該鍵をカプセル化（暗号化）した鍵カプセルＣ１を出力する。鍵Ｋと鍵カプセルＣ１は一時記憶部６０８への入力として利用される。

【００８２】

ワンタイム署名生成部６１０は、署名鍵としてワンタイム署名の署名用秘密鍵ｏｓｋを入力され、また署名対象メッセージとして、署名値ｓ１と、受信者の暗号用公開鍵ｐｋＲと、鍵カプセルＣ１と、メッセージｍと、を入力され、処理の結果として署名値ｓ２を出力する。署名値ｓ２は共通鍵暗号部６１１の入力として利用される。

【００８３】

共通鍵暗号部６１１は、暗号鍵として鍵Ｋを入力され、また暗号化対象メッセージとして署名値ｓ２およびメッセージｍを入力され、処理の結果として暗号文Ｃ２を出力する。暗号文Ｃ２は送信部６１２の入力として利用される。

【００８４】

送信部６１２は、ワンタイム署名の検証鍵ｏｖｋと、署名値ｓ１と、鍵カプセルＣ１と、暗号文Ｃ２と、が入力された後、これらを受信側装置７００へ送信する。通信にはＴＣＰ／ＩＰやＨＴＴＰ等の汎用的なプロトコルを利用可能である。

【００８５】

図７は、本実施形態に係る受信側装置７００および受信側鍵生成装置７５０の構成例を示す機能ブロック図である。

【００８６】

図７に示すように、送信側装置７００は、送信元指定部７０１、受信部７０２、記憶部７０３、鍵カプセル復号部７０４、署名検証部７０５、第一判定部７０６、共通鍵復号部７０７、ワンタイム署名検証部７０８、第二判定部７０９、出力部７１０とを含んで構成される。また、受信側鍵生成装置７５０は、暗号鍵生成部７５１を含んで構成される。

【００８７】

前述した通り、署名検証部７０５と先述の署名生成部６０４および署名鍵生成部６５１は、同じ電子署名アルゴリズムに基づく機能部である。また、ワンタイム署名検証部７０８と先述のワンタイム署名生成部６１０およびワンタイム署名鍵生成部６０１は、同じワンタイム署名方式に基づく機能部である。また、暗号鍵生成部７５１および鍵カプセル復号部７０４と、先述の鍵カプセル生成部６０７は、同一のタグ付き鍵カプセル化（ＴＢＫＥＭ）方式に基づく機能部である。

【００８８】

以下、送信元指定部７０１、記憶部７０３、受信側鍵生成装置７５０、暗号鍵生成部７５１、については、それぞれ実施形態１の送信元指定部２０１、記憶部２０３、受信側鍵生成装置２５０、暗号鍵生成部２５１、と同様の構成となるため、詳細な説明は省略する。

【００８９】

受信部７０２は、ワンタイム署名の検証鍵ｏｖｋと、署名値ｓ１と、鍵カプセルＣ１と、暗号文Ｃ２と、を送信側装置６００から受信した後、これらを必要に応じて各機能部へ転送する。受信にはＴＣＰ／ＩＰやＨＴＴＰ等の汎用的なプロトコルを利用可能である。

【００９０】

鍵カプセル復号部７０４は、タグ付き鍵カプセル復号アルゴリズムを実装した機能部で

ある。カプセル復号のための鍵として受信者の暗号用秘密鍵ｓｋＲを入力され、またタグ（補助入力）としてワンタイム署名の検証鍵ｏｖｋと、署名値ｓ１と、送信者の検証用公開鍵ｐｋＳと、を結合したものを入力され、また復号対象の鍵カプセルＣ１を入力され、処理の結果として共通鍵暗号用の鍵ＫまたはエラーコードＥＲＲを出力する。鍵ＫまたはエラーコードＥＲＲは第一判定部７０６への入力として利用される。

【００９１】

署名検証部７０５は、電子署名検証アルゴリズムを実装した機能部である。検証鍵として送信者の検証用公開鍵ｐｋＳを入力され、検証対象メッセージとしてワンタイム署名の検証鍵ｏｖｋを入力され、署名値としてｓ１を入力され、処理の結果として検証結果ｖ１（検証成功または検証失敗の二値）を出力する。検証結果ｖ１は第一判定部７０６への入力として利用される。

【００９２】

第一判定部７０６は、鍵カプセル復号部７０４の処理結果がエラーコードＥＲＲであるか、または署名検証部７０５の処理結果ｖ１が検証失敗である場合には、出力部７１０を介してエラーコードＥＲＲを受信者へ提示することで、受信した暗号文（ｏｖｋ、　ｓ１、Ｃ１、　Ｃ２）に問題があったことを示す。そうでない場合、鍵カプセル復号部７０４の処理結果である鍵Ｋを共通鍵復号部７０７へ転送する。

【００９３】

共通鍵復号部７０７は、鍵Ｋと暗号文Ｃ２を入力され、処理の結果として署名値ｓ２およびメッセージｍを出力する。署名値ｓ２およびメッセージｍはワンタイム署名検証部２０７への入力として利用される。またメッセージｍは第二判定部７０９への入力としても利用される。

【００９４】

ワンタイム署名検証部７０８は、検証鍵としてワンタイム署名の署名用検証鍵ｏｖｋを入力され、また検証対象メッセージとして署名値ｓ１と、受信者の暗号用公開鍵ｐｋＲと、鍵カプセルＣ１と、メッセージｍと、を入力され、処理の結果として検証結果ｖ２（検証成功または検証失敗の二値）を出力する。検証結果ｖ２は第二判定部７０９の入力として利用される。

【００９５】

第二判定部７０９は、ワンタイム署名検証部７０８の処理結果ｖ２が検証失敗である場合には、出力部７１０を介してエラーコードＥＲＲを受信者へ提示することで、受信した暗号文（ｏｖｋ、　ｓ１、　Ｃ１、　Ｃ２）に問題があったことを示す。そうでない場合、共通鍵復号部７０７によって復号されたメッセージｍを、出力部７１０を介して受信者へ提示する。この場合、受信者が受け取ったメッセージｍは確かに送信元指定部７０１によって指定された送信者から送られたものであることが保証される。

【００９６】

出力部７１０は、第一判定部７０６および第二判定部７０９の判定結果に基づいて受信側装置７００の利用者（受信者）へメッセージｍまたはエラーコードＥＲＲを提示する。

【００９７】

本実施形態に係る各装置（送信側装置６００、送信側鍵生成装置６５０、受信側装置７００、受信側鍵生成装置７５０）は、実施形態１と同様に、図３に示すような一般的なコンピュータ３００によって実現される。

【００９８】

次に、本実施形態における署名付き暗号文の送受信処理について、実施形態１と同様に図４を参照しながら説明する。

【００９９】

ステップ４０１からステップ４０４については実施形態１と同様であるため詳細な説明は省略する。

【０１００】

ステップ４０５では、送信側装置６００が鍵カプセルを生成する。具体的には、送信側

装置６００の鍵カプセル生成部６０７が、送信先指定部６０６の取得した送信先（受信者）の公開鍵ｐｋＲを暗号鍵として入力されるとともに、一時記憶部６０２に保存されたワンタイム署名の検証鍵ｏｖｋと、一時記憶部６０５に保存された署名値のうちｏｖｋと同じラベルをもつ署名値ｓ１と、記憶部６０３に格納された送信者の公開鍵ｐｋＳと、を結合したものをタグとして入力されることで、タグ付き鍵カプセル生成アルゴリズムに基づいて、共通鍵暗号用の鍵Ｋと、当該鍵をカプセル化した鍵カプセルＣ１と、を出力する。出力された（Ｋ、　Ｃ１）は一時記憶部６０８へ保存される。この際、ＫおよびＣ１には検証鍵ｏｖｋと同じラベルを付与して格納する。

【０１０１】

ステップ４０６については実施形態１と同様であるため詳細な説明は省略する。

【０１０２】

ステップ４０７では、送信側装置６００がワンタイム署名を生成する。具体的には、送信側装置６００のワンタイム署名生成部６１０が、一時記憶部６０２に保存されたワンタイム署名用の秘密鍵ｏｓｋを署名鍵として入力されるとともに、一時記憶部６０５によって保存された署名値のうちｏｓｋと同じラベルをもつ署名値ｓ１と、送信先指定部６０６によって取得された受信者の公開鍵ｐｋＲと、一時記憶部６０８に保存された鍵カプセルのうちｏｓｋと同じラベルをもつ鍵カプセルＣ１と、入力部６０７によって取得されたメッセージｍと、を送信対象の文書として入力されることで、ワンタイム署名生成アルゴリズムを実行し、署名値ｓ２を出力する。

【０１０３】

次に、送信側装置６００は、暗号文を生成する（ステップ４０８）。具体的には、送信側装置６００の共通鍵暗号部６１１が、一時記憶部６０８に格納された鍵のうち、ステップ４０７で利用した鍵カプセルＣ１と同じラベルを持つ鍵Ｋを選択し、暗号鍵として利用する。また、ワンタイム署名生成部６１０が生成した署名値ｓ２および入力部６０９が取得したメッセージｍを暗号化対象メッセージとして入力されることで、共通鍵暗号アルゴリズムを実行し、暗号文Ｃ２を出力する。

【０１０４】

最後に、送信側装置６００の送信部６１２が、共通鍵暗号部６１１が出力した暗号文Ｃ２と、ステップ４０７で利用した鍵カプセルＣ１と、一次記憶部６０２に保存された検証鍵のうちＣ１と同じラベルをもつ検証鍵ｏｖｋと、一時記憶部６０５に保存された署名値のうちＣ１と同じラベルをもつ署名値ｓ１と、から構成される署名付き暗号文（ｏｖｋ、ｓ１、　Ｃ１、　Ｃ２）を、ネットワークを介して受信側装置７００へ送信する（ステップ４０９）。メッセージ送信後には、ステップ４０１からステップ４０９の間に利用された鍵ペア（ｏｓｋ、　ｏｖｋ）、　署名値ｓ１、　鍵と鍵カプセル（Ｋ、　Ｃ１）はそれぞれ一時記憶部６０２、　６０５、　６０８から消去される。

【０１０５】

以上が送信側装置６００によって実行される署名付き暗号化処理の具体的な流れである。

【０１０６】

次に受信側装置７００によって実行される検証付き復号処理の具体的な流れについて説明する。受信側装置７００は、送信側装置６００によって送信された署名付き暗号文（ｏｖｋ、　ｓ１、　Ｃ１、　Ｃ２）を受信すると、まず、当該署名付き暗号文の送信者（送信側装置６００の利用者）を特定し、当該送信者の公開鍵ｐｋＳを受信側装置７００の送信元指定部７０１へ入力する（ステップ４１０）。当該公開鍵ｐｋＳは署名付き暗号文とともに送信者から送信されることもあれば、公開リポジトリなどから取得されることも可能である。

【０１０７】

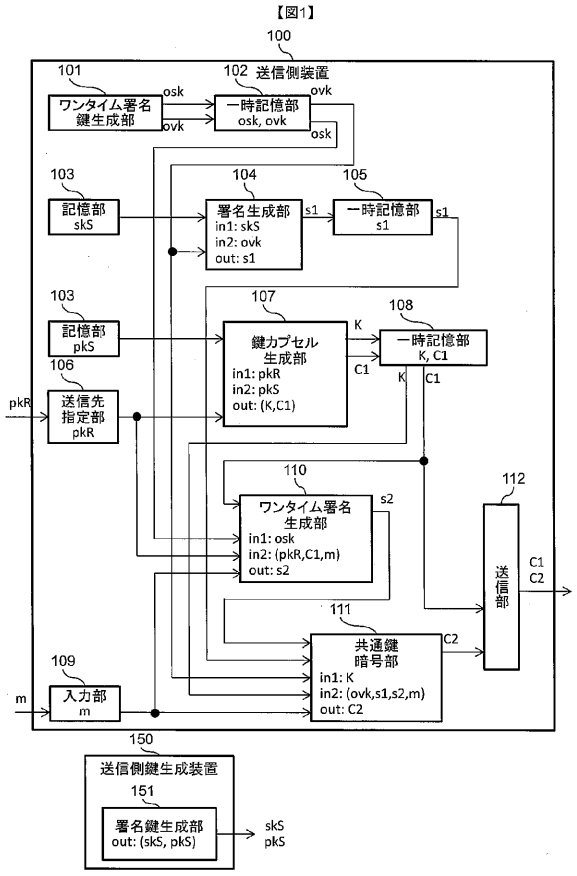
次に、受信側装置７００は、特定した送信者公開鍵ｐｋＳを元に、受信した署名付き暗号文（ｏｖｋ、　ｓ１、　Ｃ１、　Ｃ２）の検証付き復号処理を実行する（ステップ４１１）。

【０１０８】
ここで図８を用いて、当該検証付き復号処理の具体的な流れについて説明する。
【０１０９】
まず、受信側装置７００の鍵カプセル復号部７０４が、記憶部７０３に格納された受信者の秘密鍵ｓｋＲを復号鍵として入力されるとともに、受信部７０２が受信した検証鍵ｏｖｋおよび署名値ｓ１と、送信元指定部７０１が取得したｐｋＳと、を結合したものをタグとして入力され、また受信部７０２が受信したＣ１を復号対象の鍵カプセルとして入力される。鍵カプセル復号部７０４は鍵カプセル復号アルゴリズムを実行し、復号に成功した場合は鍵Ｋを出力し、失敗した場合は復号エラーを示すコードＥＲＲを出力する（ステップ８０１）。
【０１１０】
一方、受信側装置７００の署名検証部７０５は、送信元指定部７０１に格納された送信者の公開鍵ｐｋＳを検証鍵として入力されるとともに、受信部７０２によって受信されたｏｖｋを検証対象メッセージとして入力され、また同じく受信部７０２によって受信された署名値ｓ１を検証対象の署名値として入力される。署名検証部７０５は署名検証アルゴリズムを実行し、検証に成功した場合は１を、失敗した場合は０を出力する（ステップ８０２）。
【０１１１】
上記ステップ８０１および８０２に記載される二つの処理は、互いの処理結果を待つ必要がないため、並列に実行することが可能である。
【０１１２】
次に、受信側装置７００の第一判定部７０６が、鍵カプセル復号部７０４の出力と署名検証部７０５の出力に基づいて処理の継続可否を判定する（ステップ８０３）。具体的には、鍵カプセル復号部７０４が鍵Ｋの出力に成功し、かつ署名検証部７０５による検証結果が１（受理）であった場合のみ、鍵Ｋを共通鍵復号部７０７へ転送し、そうでない場合には検証エラーを示すコードＥＲＲを出力部７１０を介して受信者へ出力し、検証付き復号処理を終了する（ステップ８０８）。
【０１１３】
第一判定部７０６の判定が成功した場合、受信側装置７００の共通鍵復号部７０７が、第一判定部７０６が出力した鍵Ｋを復号用の鍵として入力されるとともに、受信部７０２が受信した暗号文Ｃ２を復号対象の暗号文として入力される。共通鍵復号部７０７は共通鍵復号アルゴリズムを実行し、復号に成功した場合は署名値ｓ２とメッセージｍを出力し、失敗した場合はエラーを示すコードＥＲＲを出力する（ステップ８０４）。
【０１１４】
次に、受信側装置７００のワンタイム署名検証部７０８が、受信部７０２が受信したｏｖｋを検証鍵として入力されるとともに、受信部７０２によって受信された署名値ｓ１と、記憶部７０３に格納された受信者の公開鍵ｐｋＲと、受信部７０２によって受信された鍵カプセルＣ１と、共通鍵復号部７０７の出力したメッセージｍと、を検証対象の文書として入力され、また共通鍵復号部７０７の出力した署名値ｓ２を検証対象の署名値として入力される。ワンタイム署名検証部７０８は、ワンタイム署名の検証アルゴリズムを実行し、検証に成功した場合は１を、失敗した場合は０を出力する（ステップ８０５）。
【０１１５】
次に、受信側装置７００の第二判定部７０９が、受信部７０２、共通鍵復号部７０７、ワンタイム署名検証部７０８、の出力に基づいて処理の継続可否を判定する（ステップ８０６）。具体的には、ワンタイム署名検証部７０８による検証結果が１（受理）であった場合のみ、メッセージｍを出力部７１０を介して受信者へ出力し（ステップ８０７）、そうでない場合には検証エラーを示すコードＥＲＲを出力部７１０を介して受信者へ出力する（ステップ８０８）。
【０１１６】
以上が受信側装置７００によって実行される検証付き復号処理の具体的な流れである。

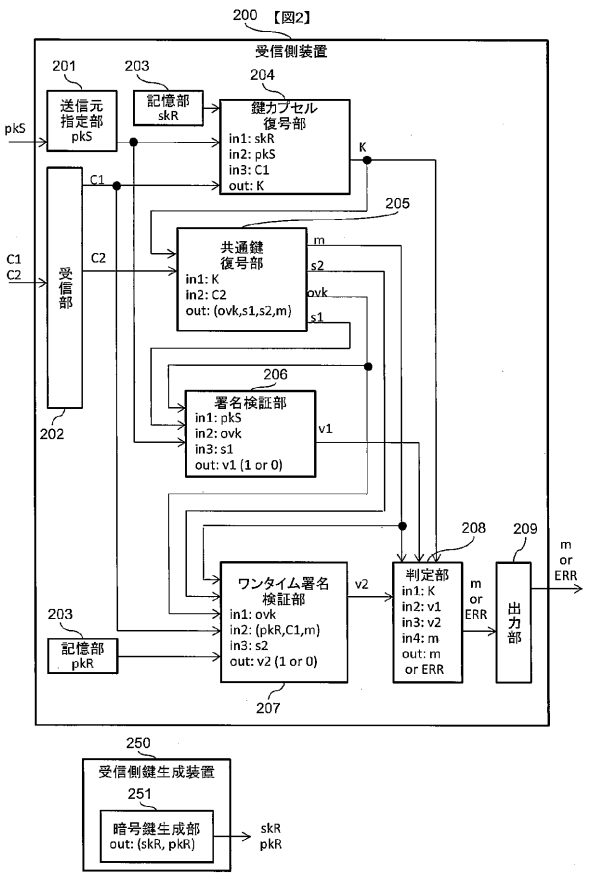
【０１１７】
以上説明したように、本実施形態に係る送信側装置６００によれば、ワンタイム署名鍵生成処理を他の処理とは独立にいつでも事前計算することが可能となる。また、送信者の署名用鍵ペア（ｓｋＳ、　ｐｋＳ）が決定した後であれば、メッセージの送信先（受信者）や送信すべきメッセージの内容が決まる前の段階であっても、署名生成処理を事前計算することが可能となる。また、送信先受信者の公開鍵ｐｋＲが決定した後であれば、送信すべきメッセージの内容が決まる前の段階でも、鍵カプセル生成処理を事前計算することが可能となる。計算コストの高い署名生成処理や鍵カプセル生成処理を事前計算しておくことで、送信すべきメッセージｍが決定された後の処理を共通鍵暗号およびワンタイム署名といった計算コストの低い処理のみで実現できるため、送信者がメッセージを決定してから暗号文が送信されるまでに要する時間を短縮することが可能となる。
【０１１８】
また、本実施形態に係る受信側装置７００によれば、鍵カプセル復号処理と電子署名検証処理の二つの処理を並列に実行することが可能となる。これにより、マルチプロセッサなどを備えた並列計算可能なハードウェアで受信側装置７００が構成される場合、非特許文献１に記載の方式に比べて処理時間の短縮が可能となる。結果として、受信者装置に暗号文が到着してから受信者がメッセージの内容を確認するまでの時間が、従来の方式、例えば非特許文献１に記載の方式に比べて短縮される。
【符号の説明】
【０１１９】
１００…送信側装置
１０１…ワンタイム署名鍵生成部
１０２…一時記憶部
１０３…記憶部
１０４…署名生成部
１０５…一時記憶部
１０６…送信先指定部
１０７…鍵カプセル生成部
１０８…一時記憶部
１０９…入力部
１１０…ワンタイム署名生成部
１１１…共通鍵暗号部
１１２…送信部
１５０…送信側鍵生成装置
１５１…署名鍵生成部
２００…受信側装置
２０１…送信元指定部
２０２…受信部
２０３…記憶部
２０４…鍵カプセル復号部
２０５…共通鍵復号部
２０６…署名検証部
２０７…ワンタイム署名検証部
２０８…判定部
２０９…出力部
２５０…受信側鍵生成装置
２５１…暗号鍵生成部
６００…送信側装置
６０１…ワンタイム署名鍵生成部
６０２…一時記憶部

６０３…記憶部
６０４…署名生成部
６０５…一時記憶部
６０６…送信先指定部
６０７…鍵カプセル生成部
６０８…一時記憶部
６０９…入力部
６１０…ワンタイム署名生成部
６１１…共通鍵暗号部
６１２…送信部
６５０…送信側鍵生成装置
６５１…署名鍵生成部
７００…受信側装置
７０１…送信元指定部
７０２…受信部
７０３…記憶部
７０４…鍵カプセル復号部
７０５…署名検証部
７０６…第一判定部
７０７…共通鍵復号部
７０８…ワンタイム署名検証部
７０９…第二判定部
７１０…出力部
７５０…受信側鍵生成装置
７５１…暗号鍵生成部

【図１】

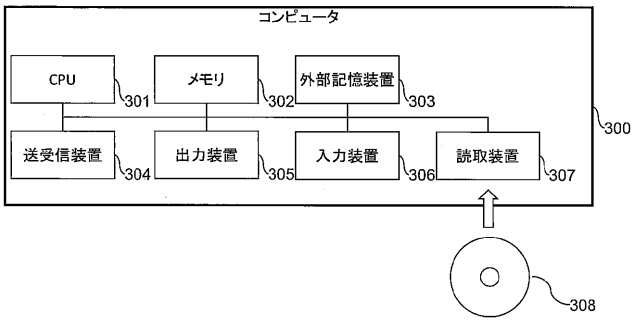


【図２】



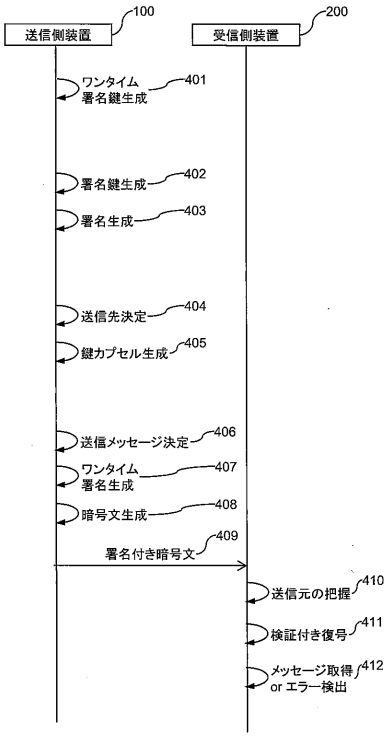
【図３】

【図3】



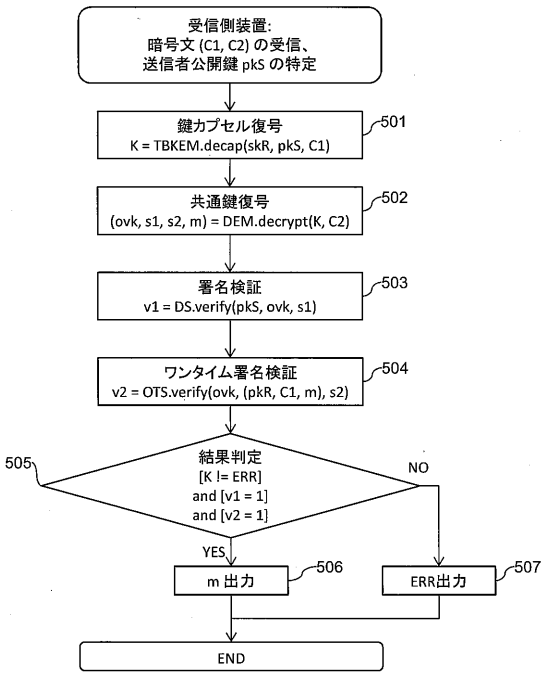
【図４】

【図4】



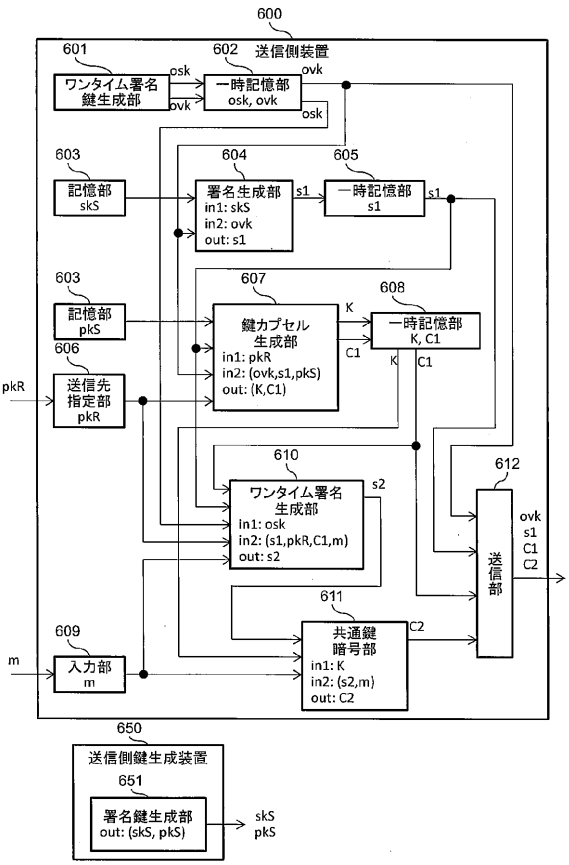
【図５】

【図5】

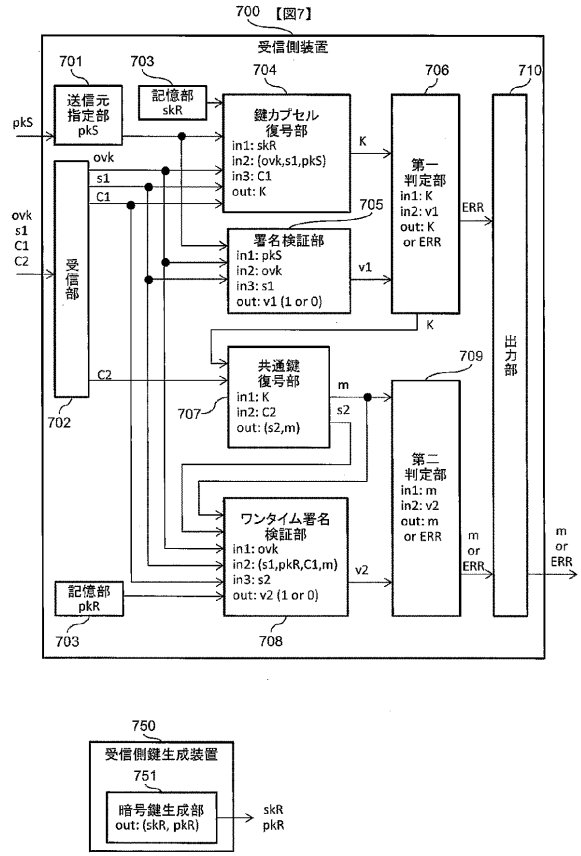


【図６】

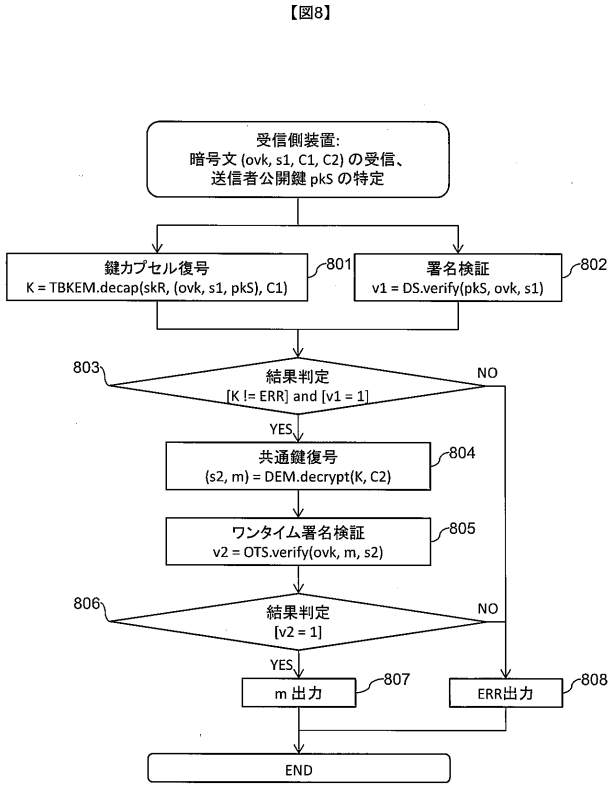
【図6】



【図７】


700 【図7】
受信側装置
701
703
704
706
710
送信元指定部 pkS
記憶部 skR
鍵カプセル復号部
in1: skR
in2: (ovk,s1,pkS)
in3: C1
out: K
第一判定部
in1: K
in2: v1
out: K or ERR
pkS
ovk
s1
C1
C2
受信部
K
ERR
出力部
705
署名検証部
in1: pkS
in2: ovk
in3: s1
out: v1 (1 or 0)
v1
K
709
共通鍵復号部
in1: K
in2: C2
out: (s2,m)
m
s2
C2
707
702
第二判定部
in1: m
in2: v2
out: m or ERR
ワンタイム署名検証部
in1: ovk
in2: (s1,pkR,C1,m)
in3: s2
out: v2 (1 or 0)
v2
m or ERR
m or ERR
記憶部 pkR
703
708
750
受信側鍵生成装置
751
暗号鍵生成部
out: (skR, pkR)
skR
pkR

【図８】


【図8】
受信側装置:
暗号文 (ovk, s1, C1, C2) の受信、
送信者公開鍵 pkS の特定
鍵カプセル復号
K = TBKEM.decap(skR, (ovk, s1, pkS), C1)
801
署名検証
v1 = DS.verify(pkS, ovk, s1)
802
803
結果判定
[K != ERR] and [v1 = 1]
NO
YES
共通鍵復号
(s2, m) = DEM.decrypt(K, C2)
804
ワンタイム署名検証
v2 = OTS.verify(ovk, m, s2)
805
806
結果判定
[v2 = 1]
NO
YES
m 出力
807
ERR出力
808
END