(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2009-296489
(P2009-296489A)
(43)公開日　平成21年12月17日(2009.12.17)

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

審査請求 未請求　請求項の数 15　ＯＬ　（全 12 頁）

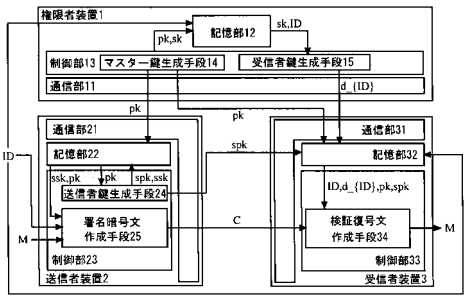
(21)出願番号　特願2008-150216 (P2008-150216)
(22)出願日　平成20年6月9日 (2008.6.9)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100084250
弁理士　丸山　隆夫
(72)発明者　寺西　勇
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5J104 AA16 EA04 EA15 EA26 JA21 NA02 NA12 NA18

(54)【発明の名称】情報処理装置、暗号化通信システム、暗号化通信方法及びプログラム

(57)【要約】
【課題】IDベース暗号の送信者が誰であるのかを偽る事ができなくなり、また、IDベース暗号の受信者が署名文を横流しできなくなる情報処理装置、暗号化通信システム、暗号化通信方法及びプログラムを提供する。
【解決手段】送信者装置は、権限者装置で生成されたマスター公開鍵を基に送信者秘密鍵及び送信者公開鍵を生成し、送信者公開鍵を受信者装置へ送信する送信者鍵生成手段と、送信者秘密鍵、受信者装置の識別情報、通信対象データを基に暗号データを作成し、受信者装置へ送信する暗号データ作成手段と、を有する。受信者装置は、権限者装置で生成された受信者秘密鍵、送信者装置から受信した送信者公開鍵及び暗号データを基に暗号データを復号し、復号結果を出力する復号結果出力手段を有する。
【選択図】図１



【特許請求の範囲】
【請求項１】
通信対象データを暗号化して受信者装置へ送信する送信者装置として機能する情報処理装置であって、
権限者装置によって生成されたマスター公開鍵に基づいて送信者秘密鍵及び送信者公開鍵を生成し、前記送信者公開鍵を前記受信者装置へ送信する送信者鍵生成手段と、
前記送信者秘密鍵と、前記受信者装置の識別情報とに基づいてデータＫ１を作成した後、前記データＫ１と、前記通信対象データとに基づいて暗号データを作成し、前記暗号データを前記受信者装置へ送信する暗号データ作成手段と、
を有することを特徴とする情報処理装置。
【請求項２】
前記暗号データ作成手段は、
前記受信者装置の識別情報のハッシュ値を計算し、
前記マスター公開鍵の一部でありかつ有限群の元である値ｈと、前記ハッシュ値とのペアリングを、前記送信者秘密鍵でべき乗したものを前記データＫ１として作成することを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記送信者鍵生成手段は、
前記マスター公開鍵の一部でありかつ有限群の元である値ｇを、前記送信者秘密鍵でべき乗したものを前記送信者公開鍵として生成することを特徴とする請求項１または２記載の情報処理装置。
【請求項４】
前記暗号データ作成手段は、
前記通信対象データに対して複数の０を連結したものを前記暗号データとして作成することを特徴とする請求項１から３のいずれか１項に記載の情報処理装置。
【請求項５】
前記マスター公開鍵は、
有限群の元である値ｇを整数ｘでべき乗したものを値ｈとし、前記値ｇと前記値ｈとを含むデータであることを特徴とする請求項１から５のいずれか１項に記載の情報処理装置。
【請求項６】
請求項１から５のいずれか１項に記載の情報処理装置で作成された暗号データを受信する受信者装置として機能する情報処理装置であって、
権限者装置によって生成された受信者秘密鍵と、前記情報処理装置によって生成された送信者公開鍵とに基づいてデータＫ２を作成した後、前記データＫ２に基づいて前記暗号データを復号し、復号結果を出力する復号結果出力手段を有することを特徴とする情報処理装置。
【請求項７】
前記復号結果出力手段は、
前記復号結果として、前記暗号データが前記通信対象データに対して複数の０を連結したものである場合には、前記通信対象データを出力し、
前記復号結果として、前記暗号データが前記通信対象データに対して複数の０を連結したものではない場合には、不正である事を表すデータを出力することを特徴とする請求項６記載の情報処理装置。
【請求項８】
前記復号結果出力手段は、
前記送信者公開鍵と、前記受信者秘密鍵とのペアリングを前記データＫ２として作成することを特徴とする請求項６または７記載の情報処理装置。
【請求項９】
前記受信者秘密鍵は、

前記受信者装置の識別情報のハッシュ値を整数ｘでべき乗したデータであることを特徴とする請求項６から８のいずれか１項に記載の情報処理装置。
【請求項１０】
請求項１から５のいずれか１項に記載の情報処理装置である送信者装置、及び、請求項６から９のいずれか１項に記載の情報処理装置である受信者装置のうち、少なくとも１つを備えることを特徴とする暗号化通信システム。
【請求項１１】
前記送信者装置及び前記受信者装置と通信を行う権限者装置をさらに備え、
前記権限者装置は、
ランダムに選んだ有限群の元である値ｇを、ランダムに選んだ整数ｘでべき乗したものを値ｈとし、前記値ｇと前記値ｈとを含むデータをマスター公開鍵として生成し、前記マスター公開鍵を前記送信者装置及び前記受信者装置へ送信するとともに、前記整数ｘを含むデータをマスター秘密鍵として生成するマスター鍵生成手段と、
前記受信者装置の識別情報のハッシュ値を計算し、前記ハッシュ値を前記マスター秘密鍵でべき乗したデータを受信者秘密鍵として生成し、前記受信者秘密鍵を前記受信者装置へ送信する受信者鍵生成手段と、
を有することを特徴とする請求項１０記載の暗号化通信システム。
【請求項１２】
通信対象データを暗号化して通信を行う暗号化通信方法であって、
マスター公開鍵に基づいて送信者秘密鍵及び送信者公開鍵を生成し、前記送信者公開鍵を受信者装置へ送信する送信者鍵生成ステップと、
前記送信者秘密鍵と、前記受信者装置の識別情報とに基づいてデータＫ１を作成した後、前記データＫ１と、前記通信対象データとに基づいて暗号データを作成し、前記暗号データを前記受信者装置へ送信する暗号データ作成送信ステップと、
を有することを特徴とする暗号化通信方法。
【請求項１３】
前記暗号データを送信者装置から受信した場合に、受信者秘密鍵と、前記送信者公開鍵とに基づいてデータＫ２を作成した後、前記データＫ２に基づいて前記暗号データを復号する暗号データ復号ステップと、
復号結果として、前記暗号データが前記通信対象データに対して複数の０を連結したものである場合には、前記通信対象データを出力し、前記復号結果として、前記暗号データが前記通信対象データに対して複数の０を連結したものではない場合には、不正である事を表すデータを出力する復号結果出力ステップと、
を有することを特徴とする請求項１２記載の暗号化通信方法。
【請求項１４】
前記マスター公開鍵は、
ランダムに選んだ有限群の元である値ｇを、ランダムに選んだ整数ｘでべき乗したものを値ｈとし、前記値ｇと前記値ｈとを含むデータであり、
前記受信者秘密鍵は、
前記受信者装置の識別情報のハッシュ値を、前記整数ｘを含むデータであるマスター秘密鍵でべき乗したデータであることを特徴とする請求項１２または１３記載の暗号化通信方法。
【請求項１５】
請求項１２から１４のいずれか１項に記載の暗号化通信方法をコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化通信システムに関し、特に、IDベース暗号を用いた情報処理装置、暗号化通信システム、暗号化通信方法及びプログラムに関する。

【背景技術】
【０００２】
インターネット等における情報通信に用いられる暗号化方式として、公開鍵暗号化方式がある。公開鍵暗号化方式は、送信者の公開鍵により情報を暗号化し、受信者の秘密鍵で復号する。この公開鍵暗号化方式は、暗号化と復号を共通の秘密鍵で行う共通鍵暗号化方式と比べて、鍵の配布や管理が容易であるというメリットがある。しかしながら、公開鍵暗号化方式は、公開鍵を証明するための電子証明書が必要である上、その有効期限の管理も必要であるので、ユーザにとっては煩雑であった。さらに、送信者の公開鍵を受信者が予め取得しておく必要があり、情報配信の自由度が妨げられていた。
【０００３】
このような不都合を解決するものとして、IDベース暗号を用いた暗号化通信（以下、IDベース暗号又はIDベース暗号方式という）がある。このIDベース暗号について以下に説明する。
【０００４】
＜IDベース暗号＞
IDベース暗号は、公開鍵暗号方式の変種であり、公開鍵としてID自身を使える方式である。この方式は、例えば特許文献１に開示されている。IDベース暗号には、権限者、ユーザの２種類のエンティティがいる。
【０００５】
IDベース暗号には、マスター鍵生成、ユーザ鍵生成、暗号化、復号の４つの手順がある。
・マスター鍵生成は権限者によって行われ、マスター公開鍵とマスター秘密鍵を出力する。
・ユーザ鍵生成は権限者によって行われ、マスター秘密鍵とIDとを入力として受け取り、IDに対応するユーザ秘密鍵を出力する。
・暗号化はユーザによって行われ、受信者のIDと平文とを入力されると暗号文を出力する。
・復号はユーザによって行われ、暗号文とIDに対応するユーザ秘密鍵とを入力されると平文を出力する。
【０００６】
上記IDベース暗号以外の暗号化方式として、「Boneh-FranklinによるIDベース暗号方式」及び「指定検証者署名」について、それぞれ以下に説明する。なお、本明細書の記載においては、「_（アンダーバー）」で添え字を表す（例えば、a_1）。また、「^」でべき乗を表す（例えば、2^3=8）。また、「Z/qZ」で0以上q未満の整数全体の集合を表す。
【０００７】
＜Boneh-FranklinによるIDベース暗号方式＞
G、Tを位数qが素数である有限巡回群とし、＜a,b＞でGの元a、bのペアリングを表す。任意のa,bに対しペアリング＜a,b＞はTの元であるものとする。ペアリングに関する詳細は非特許文献１を参照されたい。
HをGに値をとるハッシュ関数とする。
非特許文献１においてBonehとFranklinはペアリングを利用してIDベース暗号を実現している。
・マスター鍵生成ではGの元gとZ/qZの元xをランダムに選び、h=g^xを計算する。そして(g,h)をマスター公開鍵とし、xをマスター秘密鍵とする。
・ユーザ鍵生成ではIDとマスター秘密鍵xとが入力されたらd=H(ID)^xを出力する。
・暗号化ではIDと平文Mが入力されたらZ/qZの元rをランダムに選び、(u,v)=(g^r,M＜H(ID),h＞^r)を出力する。
・復号ではユーザ秘密鍵dと暗号文(u,v)とが入力されたらv/＜d,u＞を出力する。
【０００８】
＜指定検証者署名＞

指定検証者署名（指定検証者署名方式）は非特許文献２で提案されている電子署名方式の１つであり、指定検証者のみが署名文を検証できる方式である。通常の電子署名方式は誰でも署名文を検証できてしまうので、検証者が署名文を見ず知らずの第三者に横流しすると、見ず知らずの第三者に署名文を検証されてしまう危険がある。それに対し指定検証者以外の人には署名文の正当性を検証できないので、指定検証者が第三者に署名文を横流ししても、第三者に署名文を検証される危険は無い。

指定検証者署名には、署名者と検証者の２種類のエンティティがいて、署名者鍵生成、検証者鍵生成、署名、検証の４つの手順がある。

・署名者鍵生成では、署名者公開鍵と署名者秘密鍵が生成される。
・検証者鍵生成では、検証者公開鍵と検証者秘密鍵が生成される。
・署名では、署名者公開鍵と署名者秘密鍵と検証者公開鍵と文書を受け取り、署名文を出力する。
・検証では署名者公開鍵と検証者公開鍵と検証者秘密鍵と文書と署名文が入力され、「受理」を表すビット列、もしくは「拒否」を表すビット列が出力される。

非特許文献２では非特許文献３のテクニックを利用して指定検証者署名を実現している。

【特許文献１】特開２００６－３１９４５７号公報
【非特許文献１】Dan Boneh, Matthew K. Franklin, "Identity-Based Encryption from the Weil Pairing", CRYPTO 2001, pp. 213-229
【非特許文献２】Markus Jakobsson, Kazue Sako, Russell Impagliazzo, "Designated Verifier Proofs and Their Applications", EUROCRYPT 1996, pp. 143-154
【非特許文献３】R.Cramer, I.Damgard, and B.Schoenmakers, "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols",In CRYPTO'94, pp. 174-187

【発明の開示】
【発明が解決しようとする課題】
【０００９】

公開鍵暗号方式は暗号文の送信者が誰であるか分からないという欠点を持つ。この為、公開鍵暗号方式を電子署名方式と組み合わせる事で、送信者が誰であるかを偽れなくすることができる。また、署名文を横流しされては困る場合は、公開鍵暗号方式を指定検証者署名方式と組み合わせる事で、送信者が誰であるかを偽れなくすることができる。

【００１０】

しかし、IDベース暗号方式は、指定検証者署名方式と組み合わせる事で送信者が誰であるかを偽れなくする事はできない。その理由は、指定検証者署名方式は受信者の公開鍵を使わなければ作成できないが、IDベース暗号方式では受信者の公開鍵がそもそも存在しないからである。

【００１１】

本発明は、上記事情に鑑みてなされたものであり、IDベース暗号方式に指定検証者署名方式の機能を付加することにより、IDベース暗号の送信者が誰であるのかを偽る事ができなくなり、また、IDベース暗号の受信者が署名文を横流しできなくなる情報処理装置、暗号化通信システム、暗号化通信方法及びプログラムを提供することを目的とする。

【課題を解決するための手段】
【００１２】

かかる目的を達成するために、本発明の情報処理装置は、第１の態様として、通信対象データを暗号化して受信者装置へ送信する送信者装置として機能する情報処理装置であって、権限者装置によって生成されたマスター公開鍵に基づいて送信者秘密鍵及び送信者公開鍵を生成し、送信者公開鍵を受信者装置へ送信する送信者鍵生成手段と、送信者秘密鍵と、受信者装置の識別情報とに基づいてデータＫ１を作成した後、データＫ１と、通信対象データとに基づいて暗号データを作成し、暗号データを受信者装置へ送信する暗号データ作成手段と、を有することを特徴とする。

【００１３】
また、本発明の情報処理装置は、第１の態様において、暗号データ作成手段は、受信者装置の識別情報のハッシュ値を計算し、マスター公開鍵の一部でありかつ有限群の元である値ｈと、ハッシュ値とのペアリングを、送信者秘密鍵でべき乗したものをデータＫ１として作成することを特徴としてもよい。
【００１４】
また、本発明の情報処理装置は、第１の態様において、送信者鍵生成手段は、マスター公開鍵の一部でありかつ有限群の元である値ｇを、送信者秘密鍵でべき乗したものを送信者公開鍵として生成することを特徴としてもよい。
【００１５】
また、本発明の情報処理装置は、第１の態様において、暗号データ作成手段は、通信対象データに対して複数の０を連結したものを暗号データとして作成することを特徴としてもよい。
【００１６】
また、本発明の情報処理装置は、第１の態様において、マスター公開鍵は、有限群の元である値ｇを整数ｘでべき乗したものを値ｈとし、値ｇと値ｈとを含むデータであることを特徴としてもよい。
【００１７】
本発明の情報処理装置は、第２の態様として、本発明の第１の態様の情報処理装置で作成された暗号データを受信する受信者装置として機能する情報処理装置であって、権限者装置によって生成された受信者秘密鍵と、本発明の第１の態様の情報処理装置によって生成された送信者公開鍵とに基づいてデータＫ２を作成した後、データＫ２に基づいて暗号データを復号し、復号結果を出力する復号結果出力手段を有することを特徴とする。
【００１８】
また、本発明の情報処理装置は、第２の態様において、復号結果出力手段は、復号結果として、暗号データが通信対象データに対して複数の０を連結したものである場合には、通信対象データを出力し、復号結果として、暗号データが通信対象データに対して複数の０を連結したものではない場合には、不正である事を表すデータを出力することを特徴としてもよい。
【００１９】
また、本発明の情報処理装置は、第２の態様において、復号結果出力手段は、送信者公開鍵と、受信者秘密鍵とのペアリングをデータＫ２として作成することを特徴としてもよい。
【００２０】
また、本発明の情報処理装置は、第２の態様において、受信者秘密鍵は、受信者装置の識別情報のハッシュ値を整数ｘでべき乗したデータであることを特徴としてもよい。
【００２１】
本発明の暗号化通信システムは、本発明の第１の態様としての情報処理装置、及び、本発明の第２の態様としての情報処理装置のうち、少なくとも１つを備えることを特徴とする。
【００２２】
また、本発明の暗号化通信システムにおいて、送信者装置及び受信者装置と通信を行う権限者装置をさらに備え、権限者装置は、ランダムに選んだ有限群の元である値ｇを、ランダムに選んだ整数ｘでべき乗したものを値ｈとし、値ｇと値ｈとを含むデータをマスター公開鍵として生成し、マスター公開鍵を送信者装置及び受信者装置へ送信するとともに、整数ｘを含むデータをマスター秘密鍵として生成するマスター鍵生成手段と、受信者装置の識別情報のハッシュ値を計算し、ハッシュ値をマスター秘密鍵でべき乗したデータを受信者秘密鍵として生成し、受信者秘密鍵を受信者装置へ送信する受信者鍵生成手段と、を有することを特徴としてもよい。
【００２３】

本発明の暗号化通信方法は、通信対象データを暗号化して通信を行う暗号化通信方法であって、マスター公開鍵に基づいて送信者秘密鍵及び送信者公開鍵を生成し、送信者公開鍵を受信者装置へ送信する送信者鍵生成ステップと、送信者秘密鍵と、受信者装置の識別情報とに基づいてデータＫ１を作成した後、データＫ１と、通信対象データとに基づいて暗号データを作成し、暗号データを受信者装置へ送信する暗号データ作成送信ステップと、を有することを特徴とする。

【００２４】

また、本発明の暗号化通信方法において、暗号データを送信者装置から受信した場合に、受信者秘密鍵と、送信者公開鍵とに基づいてデータＫ２を作成した後、データＫ２に基づいて暗号データを復号する暗号データ復号ステップと、復号結果として、暗号データが通信対象データに対して複数の０を連結したものである場合には、通信対象データを出力し、復号結果として、暗号データが通信対象データに対して複数の０を連結したものではない場合には、不正である事を表すデータを出力する復号結果出力ステップと、を有することを特徴としてもよい。

【００２５】

また、本発明の暗号化通信方法において、マスター公開鍵は、ランダムに選んだ有限群の元である値ｇを、ランダムに選んだ整数ｘでべき乗したものを値ｈとし、値ｇと値ｈとを含むデータであり、受信者秘密鍵は、受信者装置の識別情報のハッシュ値を、整数ｘを含むデータであるマスター秘密鍵でべき乗したデータであることを特徴としてもよい。

【００２６】

本発明のプログラムは、本発明の暗号化通信方法をコンピュータに実行させることを特徴とする。

【発明の効果】

【００２７】

本発明によれば、IDベース暗号の送信者が誰であるのかを偽る事ができなくなる。またIDベース暗号の受信者が署名文を横流しできなくなる。

【発明を実施するための最良の形態】

【００２８】

以下、本発明を実施するための最良の形態について添付図面を参照して詳細に説明する。

【００２９】

図１は、本発明の一実施形態である暗号化通信システムの構成を示す図である。図１に示すように、本実施形態の暗号化通信システムは、インターネット等のネットワークを介して接続される、権限者装置１と、送信者装置２と、受信者装置３とを有する。これら各装置は、プログラム制御により所定の情報処理を行う、本発明の一実施形態としての情報処理装置である。プログラムの例としては、上述したIDベース暗号方式や指定検証者署名方式を行うためのプログラムの他に、後述する本発明の一実施形態である暗号化通信方法を行うためのプログラムが挙げられる。また、送信者装置２と、受信者装置３とは複数存在してもよい。

【００３０】

図１に示す暗号化通信システムにおいて、送信者装置２は、受信者装置３に対して、所定の情報（電子データ、通信対象データ）を送信する。情報の例としては、電子メール等が挙げられる。

【００３１】

権限者装置１は、通信部１１と、記憶部１２と、制御部１３とを有する。制御部１３は、マスター鍵生成手段１４と、受信者鍵生成手段１５とを有する。

【００３２】

送信者装置２は、通信部２１と、記憶部２２と、制御部２３とを有する。制御部２３は、送信者鍵生成手段２４と、署名暗号文作成手段２５とを有する。

【００３３】

受信者装置３は、通信部３１と、記憶部３２と、制御部３３とを有する。制御部３３は、検証復号文作成手段３４を有する。

【００３４】

通信部１１、２１、３１は、通信用のインターフェースデバイスで実現される。例えば、インターネットに接続可能なモデム等が利用できる。記憶部１２、２２、３２は、記憶デバイスや記憶媒体で実現される。例えばハードディスクやメモリ等が利用できる。制御部１３、２３、３３は、制御デバイスで実現される。例えばＣＰＵ（Central Processing Unit）等が利用できる。各記憶部には、上述したプログラムが格納されており、各ＣＰＵは、各プログラムに従って各部（各手段）を制御し、本実施形態の暗号化通信方法を実行する。また、各記憶部には、その装置自身のID（識別情報）が予め格納されているものとする。

【００３５】

受信者装置３には、IDが振られていて、そのIDはシステム上の全ての装置に公知であるとする。

【００３６】

次に、図１を参照しながら、上記各制御部１３、２３、３３における各手段の入出力を説明する。なお図１において、矢印の向かう方向が「出力先」となる。

【００３７】

権限者装置１において、マスター鍵生成手段１４は、マスター公開鍵pkとマスター秘密鍵skとを出力する。また、受信者鍵生成手段１５は、マスター秘密鍵skと受信者装置３のIDを入力として受け取り、そのIDに対応する受信者秘密鍵d_[ID]を出力する。

【００３８】

送信者装置２において、送信者鍵生成手段２４は、マスター公開鍵pkを入力として受け取り、送信者公開鍵spkと送信者秘密鍵sskを出力する。また、署名暗号文作成手段２５は、マスター公開鍵pk、送信者秘密鍵ssk、受信者装置３のID、平文M（通信対象データの一例）を入力として受け取り、署名暗号文C（暗号データの一例）を出力する。

【００３９】

受信者装置３において、検証復号文作成手段３４は、マスター公開鍵pk、送信者公開鍵spk、受信者装置３自身のID、受信者秘密鍵d_[ID]、署名暗号文Cを入力として受け取り、復号結果として、平文Mを出力するか、あるいは、「拒否」を表すビット列（不正であることを示すデータ）を出力する。

【００４０】

なお、本実施形態では、説明の便宜上、送信者装置２と受信者装置３とを分け、各装置の構成を別々のものとしたが、送信者装置２が受信者装置に、また、受信者装置３が送信者装置になりうることは言うまでもない。従って、各制御部２３、３３はそれぞれ、送信者鍵生成手段２４、署名暗号文作成手段２５、検証暗号文作成手段３４を全て有するように構成してもよい。

【００４１】

次に、本実施形態である暗号化通信システムの動作（本発明の一実施形態である暗号化通信方法）の流れについて、図２を参照して説明する。

【００４２】

権限者装置１において、マスター鍵生成手段１４は、マスター公開鍵pkとマスター秘密鍵skを生成し、記憶部１２に書き込む（ステップＳ１）。そして、マスター鍵生成手段１４は、通信部１１を介して、マスター公開鍵pkを送信者装置２及び受信者装置３に送信し、公開する（ステップＳ２、Ｓ３）。ここで、公開方法はどのようなものを用いてもよいが、例として、ＰＫＩ（Public Key Infrastructure）を利用する、あるいは、公開掲示板に載せる、という方法が挙げられる。

【００４３】

送信者装置２において、通信部２１がマスター公開鍵pkを受信すると、そのマスター公開鍵pkは記憶部２２に書き込まれる（ステップＳ４）。同様に、受信者装置３において、

通信部３１がマスター公開鍵pkを受信すると、マスター公開鍵pkは記憶部３２に書き込まれる（ステップＳ５）。

【００４４】

ここで、各々の受信者装置３にはIDが割り振られており、各IDは何らかの手段（方法）により他装置に公知になっているとする。受信者装置３において、通信部３１を介して、受信者装置３自身のIDが権限者装置１に送信される（ステップＳ６）。

【００４５】

権限者装置１において、通信部１１が受信者装置３のIDを受信すると、そのIDは記憶部１２に書き込まれる（ステップＳ７）。また、受信者鍵生成手段１５は、マスター秘密鍵sk及び受信者装置３のIDを記憶部１２から読み出す。そして、受信者鍵生成手段１５は、マスター秘密鍵sk及び受信者装置３のIDに基づいて、受信者秘密鍵d_[ID]を生成する（ステップＳ８）。生成された受信者秘密鍵d_[ID]は、通信部１１を介して、受信者装置３に送られる（ステップＳ９）。

【００４６】

受信者装置３において、通信部３１が受信者秘密鍵d_[ID]を受信すると、その受信者秘密鍵d_[ID]は記憶部３２に書き込まれる（ステップＳ１０）。

【００４７】

送信者装置２において、送信者鍵生成手段２４は、記憶部２２に書き込まれているマスター公開鍵pkを読み出す。そして、送信者鍵生成手段２４は、読み出したマスター公開鍵pkに基づいて送信者公開鍵spkと送信者秘密鍵sskを生成し、記憶部２２に書き込む（ステップＳ１１）。また、送信者鍵生成手段２４は、通信部２１を介して、送信者公開鍵spkを受信者装置３に送信し、公開する（ステップＳ１２）。

【００４８】

受信者装置３において、通信部３１が送信者公開鍵spkを受信すると、その送信者公開鍵spkは記憶部３２に書き込まれる（ステップＳ１３）。

【００４９】

受信者装置３のIDと平文M（通信対象データの一例）とを送信者装置２に入力する事で、平文Mの署名暗号文Cを作成できる。送信者装置２において、受信者装置３のIDと平文Mが入力されると（ステップＳ１４）、署名暗号文作成手段２５は、マスター公開鍵pkと送信者秘密鍵sskを記憶部２２から読み出す。署名暗号文作成手段２５は、読み出したマスター公開鍵pk及び送信者秘密鍵sskと、入力された受信者装置３のID及び平文Mとに基づいて、署名暗号文Cを生成する（ステップＳ１５）。そして、署名暗号文作成手段２５は、通信部２１を介して、署名暗号文Cを受信者装置３に送信する（ステップＳ１６）。

【００５０】

受信者装置３において、通信部３１が署名暗号文Ｃを受信すると、検証復号文作成手段３４は、記憶部３２から、マスター公開鍵pk、送信者公開鍵spk、受信者装置３自身のID、受信者秘密鍵d_[ID]を読み出す。そして、検証復号文作成手段３４は、署名暗号文C、マスター公開鍵pk、送信者公開鍵spk、受信者装置３のID、受信者秘密鍵d_[ID]に基づいて、署名暗号文Cの復号を行う（ステップＳ１７）。そして、検証復号文作成手段３４は、復号結果を出力（例えば、画面表示や印刷）する（ステップＳ１８）。復号結果は、平文Mそのまま、あるいは、不正であることを示すデータのいずれかである。また、検証復号文作成手段３４は、復号結果を記憶部３２に書き込むようにしてもよい。

【００５１】

次に、上述した本実施形態の暗号化通信システムの動作の具体例（上記各手段の詳細）について説明する。

【００５２】

G、Tを位数qが素数である有限巡回群とし、＜a,b＞でGの元a、bのペアリングを表す。任意のa,bに対しペアリング＜a,b＞はTの元であるものとする。ペアリングに関する詳細は非特許文献１を参照されたい。HをGに値をとるハッシュ関数し、E、Dをそれぞれ共通鍵暗号方式の暗号化関数と復号関数とする。安全性上の観点から言えば、qは160ビット以上

にするのが望ましい。

【００５３】

本実施形態では共通鍵暗号を利用するが、安全性上の理由により、この共通鍵暗号は「不正な方法で鍵を作成した場合には、復号アルゴリズムが「不正」を表す文字列を出力する」という性質を満たすものでなければならない。

【００５４】

公開鍵系のプリミティブを共通鍵暗号と組み合わせるというテクニックはハイブリッド暗号や鍵共有で頻繁に使われているものだが、この「不正」を表す文字列を出力するという要件を要求するところが本実施形態の特徴である。本実施形態は、指定検証者署名の機能を持っているので、作成された署名が不正なものかどうかを判定する必要があり、復号アルゴリズムが「不正」を出力するかどうかによって署名が不正かどうかを判定する。

【００５５】

AESやDESのようなブロック暗号は「不正」を表す文字列を出力しないので、本実施形態ではこれらを改良したものを使う。E',D'を何らかの共通鍵暗号方式Π’の暗号化関数と復号関数とする。たとえばΠ’としてDESやAESを使えるが、どのようなものを用いてもよい。Πはnビット(nは自然数)の平文を暗号化できるとする。さらにkをn以下の自然数とする。kは大きければ大きいほど安全性が高まる。

【００５６】

暗号方式は、例えば次の方法で作成できる。E',D',kを用いて、n-kビットの平文Mを暗号化できる共通鍵暗号方式Πの暗号化関数Eと復号関数Dを作る。E(M,K)はMのあとに0をk個並べたビット列M'を作り、C=E'(M',K)を計算して署名暗号文Cを出力する。D(C,K)はM'=D'(C,K)を計算し、M'の後ろkビットが全て0であるならM'の前n-kビット、すなわち平文Mを出力し、そうでなければ⊥、すなわち「不正」を表す文字列を出力する。

【００５７】

マスター鍵生成手段１４では、Gの元gとZ/qZの元xをランダムに選び、h=g^xを計算する。そして(g,h)をマスター公開鍵として出力し、xをマスター秘密鍵として出力する。すなわち、マスター鍵生成手段１４は、有限群の元g及び整数xをランダムに選び、gをxでべき乗したものをhとし、gとhとを含むデータをマスター公開鍵(g,h)とし、また、xを含むデータをマスター秘密鍵xにする。

【００５８】

受信者鍵生成手段１５では、マスター秘密鍵xと、受信者装置３のIDとが入力されたら、まず受信者装置３のIDのハッシュ値を計算する。次に、受信者鍵生成手段１５は、d=H(ID)^xを計算し、dを受信者秘密鍵として出力する。上記受信者秘密鍵dは、受信者装置３のIDのハッシュ値をマスター秘密鍵xでべき乗したものである。

【００５９】

送信者鍵生成手段２４は、マスター公開鍵(g,h)が入力されたら、qZの元yをランダムに選び、h_Y=g^yを計算し、h_Yを送信者公開鍵として出力し、yを送信者秘密鍵として出力する。

【００６０】

署名暗号文作成手段２５では、マスター公開鍵(g,h)と、受信者装置３のIDと、送信者秘密鍵yと、平文Mとが入力されたら、まず受信者装置３のIDのハッシュ値を計算する。次に、署名暗号文作成手段２５は、K1=＜H(ID),h＞^yを計算する。このK1は、マスター公開鍵(g,h)の一部でありかつ有限群の元であるhと、受信者装置３のIDのハッシュ値とのペアリングを、送信者秘密鍵ｙでべき乗したものである。次に、署名暗号文作成手段２５は、C=E(M,K1)を計算し、Cを署名暗号文として出力する。

【００６１】

検証復号文作成手段３４では、送信者公開鍵h_Yと、受信者秘密鍵dと、署名暗号文Cとが入力されたら、まずK2=＜d,h_Y＞を計算し、次にM＝D(C,K2)を計算する。そして、復号結果として、M＝⊥なら「不正（拒否）」を表す文字列を出力し、そうでなければ平文Mを出力する。すなわち、検証復号文作成手段３４は、復号結果として、署名暗号文Cが平文M

に対して複数の０を連結したものである場合には平文Mを出力し、その一方で、署名暗号文Cが平文Mに対して複数の０を連結したものではない場合には、不正である事を表すデータを出力する。出力の例としては、上述したように画面表示や印刷等が挙げられる。また、復号結果を記憶部３２等に記憶するようにしてもよい。

【００６２】

上述したBoneh-FranklinのIDベース暗号方式との違いの一つは、h_Y=g^yの作り方である。Boneh-FranklinのIDベース暗号方式では、暗号文作成者がg^yを作成するのに対し、本実施形態では受信者がg^yを作成する。しかもBoneh-FranklinのIDベース暗号方式では、yとh_Yはテンポラリなデータで暗号化のたびにyを選びなおしてh_Y=g^yを計算するのに対し、本実施形態では、yとh_Yはそれぞれ受信者の秘密鍵と公開鍵で一度h_Y=g^yを作成したらそれを使い続ける。

【００６３】

以上、本発明の実施形態について説明したが、上記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々の変形が可能である。

【００６４】

例えば、上述した本実施形態における各装置１～３の動作は、ハードウェア、または、ソフトウェア、あるいは、両者の複合構成によって実行することも可能である。

【００６５】

ソフトウェアによる処理を実行する場合には、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれているコンピュータ内のメモリにインストールして実行させてもよい。あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させてもよい。

【００６６】

例えば、プログラムは、記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことが可能である。あるいは、プログラムは、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)、ＭＯ(Magneto optical)ディスク、ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的、あるいは、永続的に格納（記録）しておくことが可能である。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することが可能である。

【００６７】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送してもよい。または、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送してもよい。コンピュータでは、転送されてきたプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることが可能である。

【００６８】

また、上記実施形態で説明した処理動作に従って時系列的に実行されるのみならず、処理を実行する装置の処理能力、あるいは、必要に応じて並列的にあるいは個別に実行するように構築することも可能である。

【００６９】

また、上記実施形態で説明したシステムは、複数の装置の論理的集合構成にしたり、各装置の機能を混在させたりするように構築することも可能である。

【図面の簡単な説明】

【００７０】

【図１】本発明の実施形態である暗号化通信システムの構成を示す図である。

【図２】本発明の実施形態である暗号化通信システムの動作を示すシーケンスチャートである。

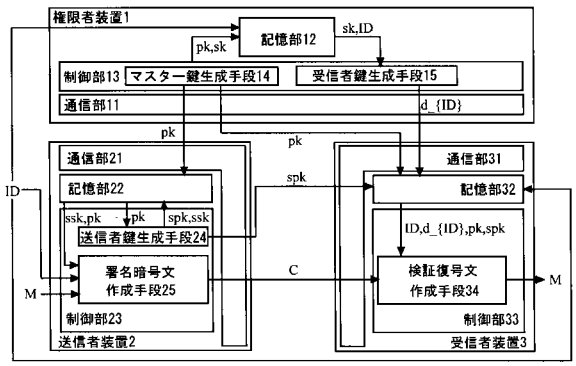
【符号の説明】

【００７１】

１　　権限者装置

２　送信者装置
３　受信者装置
１１　通信部
１２　記憶部
１３　制御部
１４　マスター鍵生成手段
１５　受信者鍵生成手段
２１　通信部
２２　記憶部
２３　制御部
２４　送信者鍵生成手段
２５　署名暗号文作成手段（暗号データ作成手段の一例）
３１　通信部
３２　記憶部
３３　制御部
３４　検証暗号文作成手段（復号結果出力手段の一例）

【図１】



pk：マスター公開鍵
sk：マスター秘密鍵
d_{ID}：受信者秘密鍵
spk：送信者公開鍵
ssk：送信者秘密鍵
M：平文
C：署名暗号文
ID：受信者装置３のＩＤ

【図２】

