

## 明 細 書

発明の名称：

携帯可能電子装置、情報処理装置、情報処理システム、及び情報処理方法  
技術分野

[0001] 本発明の実施形態は、携帯可能電子装置、情報処理装置、情報処理システム、及び情報処理方法に関する。

### 背景技術

[0002] IC (Integrated Circuit) チップを備えたICカードなどのセキュリティデバイスが、広く普及し、クレジットカードやIC旅券として利用されている。ICカードは、利用者に携帯されることから、携帯可能電子装置などと呼ばれている。

[0003] 例えば、IC旅券と読み取り装置の双方は、毎回、楕円暗号鍵を生成し、双方の公開鍵を交換し、以降の処理を暗号化して通信するためのセッション鍵を生成する。このセッション鍵は、秘匿性、完全性を確保するために利用されており、暗号化するだけでなく、認証子を生成するためにも利用される。旅券においては、暗号化用及び認証子用のセッション鍵が同時に生成され共有される。この方式では、公開鍵のみが交換されるため、セッション鍵の特定は非常に困難になっている。

### 先行技術文献

#### 特許文献

[0004] 特許文献1：日本国特表2022-537733号公報

特許文献2：国際公開第2021/029173号

特許文献3：日本国特許7004654号公報

### 発明の概要

#### 発明が解決しようとする課題

[0005] 量子計算機の出現により、量子計算機で計算が困難とされる暗号 (Post Quantum Cryptography: PQC (耐量子計算機暗号)) への移行が必要となり

つつある。そのような状況の中、ＩＣカードなどのセキュリティデバイスは、安全性は非常に高いものの、ＰＱＣを搭載する上では、読み取り装置と比較して、揮発性メモリ及び不揮発性メモリが小さく、ＣＰＵ（Central Processing Unit）の計算速度も十分ではない。すなわち、ＩＣカードのハードウェアリソースが、ＰＱＣを搭載することのハードルとなっている。このようなハードウェアリソースが厳しいデバイスについて、ＰＱＣ等の所定の暗号アルゴリズムの搭載を可能とする技術が要望されている。

[0006] 本発明が解決しようとする課題は、限られたハードウェアリソースにて所定の暗号アルゴリズムの搭載を可能とする携帯可能電子装置、情報処理装置、情報処理システム、及び情報処理方法を提供することである。

#### 課題を解決するための手段

[0007] 実施形態に係る携帯可能電子装置は、メモリ、インタフェース、及びプロセッサを備える。前記メモリは、暗号アルゴリズムを含む暗号情報を記憶する。前記インタフェースは、情報処理装置と通信する。前記プロセッサは、乱数を生成する。また、前記インタフェースは、前記暗号情報を前記情報処理装置へ送信し、前記暗号アルゴリズムに基づき生成される公開鍵及び秘密鍵のうちの前記情報処理装置から送信される前記公開鍵を受信する。前記プロセッサは、前記公開鍵に基づく暗号化処理により前記乱数から暗号化乱数を生成する。前記インタフェースは、前記暗号化乱数を前記情報処理装置へ送信する。前記プロセッサは、前記乱数に基づき前記情報処理装置との通信に使用するセッション鍵を生成する。

#### 図面の簡単な説明

[0008] [図1]図1は、実施形態に係る携帯可能電子装置としてのＩＣカード、及びＩＣカードと通信する情報処理装置としてのＩＣカード処理装置を備える情報処理システムの一例を示すブロック図である。

[図2]図2は、実施形態に係るＩＣカードの構成例を概略的に示すブロック図である。

[図3]図3は、実施形態に係るセッション鍵共有処理シーケンスの第1例を示

す図である。

[図4]図4は、実施形態に係るセッション鍵共有処理シーケンスの第2例を示す図である。

[図5]図5は、実施形態に係るセッション鍵共有処理シーケンスの第3例を示す図である。

[図6]図6は、実施形態に係るセッション鍵共有処理シーケンスの第4例を示す図である。

[図7]図7は、実施形態に係るセッション鍵共有処理シーケンスの第5例を示す図である。

[図8]図8は、実施形態に係るセッション鍵共有処理シーケンスの第6例を示す図である。

[図9]図9は、PQC標準方式 (Kyber) のAlgorithm 1の例示である。

[図10]図10は、PQC標準方式 (Kyber) のAlgorithm 2の例示である。

### 実施形態

[0009] 以下、実施形態について、図面を参照しながら説明する。

図1は、実施形態に係る携帯可能電子装置としてのICカード、及びICカードと通信する情報処理装置としてのICカード処理装置を備える情報処理システムの一例を示すブロック図である。

図1に示すように、情報処理システムは、ICカード処理装置1及びICカード2を備える。ICカード処理装置1は、ICカード2へコマンドを供給し、ICカード2からのレスポンスを受け取る上位装置である。

[0010] 図1に示す構成例において、ICカード処理装置1は、CPU (Central Processing Unit) 11、ディスプレイ12、操作部13、カードリーダライタ14、OCR (Optical Character Recognition又はOptical Character Reader) 15、及び記憶部16を備える。

[0011] CPU 11は、ICカード処理装置1全体の動作を制御するプロセッサである。CPU 11は、記憶部16に記憶されている制御プログラム及び制御データに基づいて種々の処理を行う。例えば、CPU 11は、記憶部16等

のメモリに記憶されているプログラムを実行することにより、ＩＣカード処理装置１の動作制御あるいはＩＣカード処理装置１の運用形態に応じた種々の処理を行う。なお、各種の機能のうちの一部は、ハードウェア回路により実現されるものであっても良い。この場合、ＣＰＵ１１は、ハードウェア回路により実行される機能を制御する。

[0012] 例えば、ＣＰＵ１１は、カードリーダーライタ１４を介してＩＣカード２から送信される暗号情報を取得し、暗号情報に含まれるＰＱＣ暗号アルゴリズム及び鍵長に基づき、ＰＱＣの鍵ペアである公開鍵（Pub Key）及び秘密鍵（Sec Key）を生成する機能を有する。また、ＣＰＵ１１は、カードリーダーライタ１４を介してＩＣカード２へ公開鍵又は暗号化公開鍵等の各種データを送信する機能を有する。また、ＣＰＵ１１は、カードリーダーライタ１４を介してＩＣカード２へ送信する公開鍵等の各種データを暗号化する機能を有する。また、ＣＰＵ１１は、カードリーダーライタ１４を介してＩＣカード２から送信される暗号化乱数等の各種暗号化データを復号する機能を有する。また、ＣＰＵ１１は、復号された乱数に基づきセッションキー等を生成する機能を有する。また、ＣＰＵ１１は、カードリーダーライタ１４を介して操作部１３の入力に基づき動作してもよい。例えば、ＣＰＵ１１は、操作部１３で入力されたデータを含む書き込みコマンドをＩＣカード２に送信することにより、ＩＣカード２に当該データの書き込み処理を要求する。なお、本実施形態では、ＰＱＣ暗号アルゴリズムを搭載するケースについて説明するが、ＰＱＣ暗号アルゴリズムに限定されるものではなく、本実施形態の仕組みは、所定の暗号アルゴリズムに適用可能である。

[0013] ディスプレイ１２は、ＣＰＵ１１の制御により種々の情報を表示する表示装置である。ディスプレイ１２は、例えば、液晶モニタなどである。

[0014] 操作部１３は、ＩＣカード処理装置１の利用者によって、種々の操作指示及びデータなどが入力される。操作部１３は、入力された操作指示及びデータなどをＣＰＵ１１へ送信する。操作部１３は、例えば、キーボード、テンキー、及び、タッチパネルなどである。

- [0015] カードリーダライタ 14 は、ＩＣカード 2 と通信するインタフェース（第 2 のインタフェース）である。カードリーダライタ 14 は、ＩＣカード 2 の所定の通信プロトコル等に応じたインタフェースにより構成される。
- [0016] 例えば、ＩＣカード 2 が接触型のＩＣカードである場合、例えば、ISO/IEC 7816 に準拠し、カードリーダライタ 14 は、ＩＣカード 2 の接触部と物理的かつ電氣的に接続するための接触部などにより構成される。また、ＩＣカード 2 が非接触型のＩＣカードである場合、例えば、ISO/IEC 14443 に準拠し、カードリーダライタ 14 は、ＩＣカード 2 との無線通信を行うためのアンテナおよび通信制御部などにより構成される。
- [0017] また、ＩＣカード 2 が、接触型及び非接触型の両方をサポートするデュアルカードである場合、ＩＣカード処理装置 1 のカードリーダライタ 14 は、デュアルカードに対応する構成となる。即ち、カードリーダライタ 14 は、ＩＣカード 2 の通信部 25 と物理的かつ電氣的に接触して信号の送受信を行うための通信制御部と接触部、及びＩＣカード 2 の通信部 25 との無線通信を行うための変復調回路などの通信制御部とアンテナにより構成される。
- [0018] また、カードリーダライタ 14 は、ＩＣカード 2 に対する電源供給、クロック供給、リセット制御、データの送受信を行う。例えば、カードリーダライタ 14 は、ＣＰＵ 11 による制御に基づいてＩＣカード 2 を活性化（起動）し、種々のコマンドを送信し、送信したコマンドに対する応答（レスポンス）を受信する。
- [0019] ＯＣＲ 15 は、ＩＣカード 2 から情報を取得するインタフェース（外部インタフェース）である。ＩＣカード 2 には、文字と数字と記号の組み合わせ、バーコード、又はＱＲコード（登録商標）など、光学的に読み取り可能な情報が印刷されており、ＯＣＲ 15 は、この情報を光学的に読み取り、読み取り結果をＣＰＵ 11 へ出力する。例えば、ＣＰＵ 11 は、読み取り結果に基づき復号処理により暗号化乱数から乱数を生成する。
- [0020] ＩＣカード処理装置 1 は、カードリーダライタ 14 とＯＣＲ 15 を備えることにより、これら独立した二つの経路を介して、ＩＣカード 2 から情報を

取得する。

[0021] 記憶部 16 は、不揮発性及び揮発性のメモリを備え、不揮発性のメモリは、予め制御用のプログラム、及び制御データなどを記憶し、揮発性のメモリは、CPU 21 の処理中のデータなどを一時的に格納したり、受信用バッファ、計算用バッファ、送信用バッファとして機能したりする。

[0022] 次に、ICカード 2 について説明する。

ICカード 2 は、ICカード処理装置 1 などの上位装置から電力などの供給を受けて活性化され、動作可能な状態になる。例えば、ICカード 2 が接触型の通信により ICカード処理装置 1 と接続される場合、つまり、ICカード 2 が接触型の ICカードで構成される場合、ICカード 2 は、通信インタフェースとしての接触部を介して ICカード処理装置 1 からの動作電源及び動作クロックの供給を受けて活性化される。

[0023] また、ICカード 2 が非接触型の通信方式により ICカード処理装置 1 と接続される場合、つまり、ICカード 2 が非接触式の ICカードで構成される場合、ICカード 2 は、通信インタフェースとしてのアンテナ及び変復調回路などを介して ICカード処理装置 1 からの電波を受信し、その電波から電源部により動作電源及び動作クロックを生成して活性化するようになっている。

[0024] また、ICカード 2 は、カードの片面又は両面に MRZ (Machine Readable Zone) 20 を備え、MRZ は、文字と数字と記号の組み合わせ、バーコード、又は QRコードなど、光学的に読み取り可能な印刷情報を含む。

[0025] 次に、ICカード 2 の構成例について説明する。

図 2 は、実施形態に係る ICカードの構成例を概略的に示すブロック図である。

ICカード 2 は、プラスチックなどで形成されたカード状の本体 C を有する。ICカード 2 は、本体 C 内にモジュール M が内蔵されている。モジュール M は、1 つまたは複数の ICチップ C a と通信用の外部インタフェースとが接続された状態で一体的に形成され、ICカード 2 の本体 C 内に埋設され

ている。また、ＩＣカード２のモジュールＭは、図２に示すように、ＣＰＵ ２１、ＲＯＭ ２２、ＲＡＭ ２３、ＮＶＭ ２４、通信部 ２５を備えている。これらの各部は、データバスを介して互いに接続されている。

[0026] ＣＰＵ ２１は、ＩＣカード２全体の制御を司る制御部として機能するプロセッサである。ＣＰＵ ２１は、ＲＯＭ ２２あるいはＮＶＭ ２４に記憶されている制御プログラム及び制御データに基づいて種々の処理を行う。例えば、ＣＰＵ ２１は、ＲＯＭ ２２に記憶されているプログラムを実行することにより、ＩＣカード２の動作制御あるいはＩＣカード２の運用形態に応じた種々の処理を行う。なお、各種の機能のうちの一部は、ハードウェア回路により実現されるものであっても良い。この場合、ＣＰＵ ２１は、ハードウェア回路により実行される機能を制御する。

[0027] 例えば、ＣＰＵ ２１は、ＲＯＭ ２２から暗号情報を読み出し、通信部 ２５を介して、ＩＣカード２がサポートするＰＱＣ暗号アルゴリズム及び鍵長を含む暗号情報をＩＣカード処理装置１へ送信する機能を有する。また、ＣＰＵ ２１は、ＩＣカード処理装置１から送信される公開鍵に基づく暗号化処理により、乱数から暗号化乱数を生成する機能を有する。また、ＣＰＵ ２１は、通信部 ２５を介して、暗号化乱数をＩＣカード処理装置１へ送信する機能を有する。また、ＣＰＵ ２１は、乱数に基づきセッションキー等を生成する機能を有する。

[0028] ＲＯＭ ２２は、予め制御用のプログラム、制御データ、暗号情報、及び識別情報などを記憶する不揮発性のメモリである。ＲＯＭ ２２は、製造段階で制御プログラム及び制御データなどを記憶した状態でＩＣカード２に組み込まれる。即ち、ＲＯＭ ２２に記憶されるプログラム、制御データ、暗号情報、及び識別情報は、予めＩＣカード２の仕様に応じて組み込まれる。なお、ＲＯＭ ２２は、フラッシュメモリによって構成されていてもよく、製造段階で、書き込みを行ってもよいし、その後のフェーズにおいて、書き込み及び書き換えを行うことも出来る。暗号に関する情報は、製造段階で書き込むことも可能であるが、その後のフェーズで書き込み及び更新を行ってもよい。

- [0029] 暗号情報は、ＩＣカード２によりサポートされるＰＱＣ暗号アルゴリズム及び鍵長を含む。識別情報は、ＩＣカード２を識別可能な固有の情報である。ＭＲＺ２０は、文字と数字と記号の組み合わせ、バーコード、又はＱＲコードなど光学的に読み取り可能な印刷情報として識別情報を含む。なお、ＭＲＺ２０は、識別情報の全てを含んでもよいし、識別情報の一部を含んでもよい。ＭＲＺ２０が、識別情報を含む形態としては、印刷以外の形態であってもよい。例えば、識別情報が、文字と数字と記号の組み合わせであれば、ＭＲＺ２０が、これら識別情報に対応するエンボス加工を含んでもよい。
- [0030] ＲＡＭ２３は、揮発性のメモリである。ＲＡＭ２３は、ＣＰＵ２１の処理中のデータなどを一時的に格納する。例えば、ＲＡＭ２３は、受信用バッファ、計算用バッファ、送信用バッファなどを備える。受信用バッファは、ＩＣカード処理装置１から送信され通信部２５を介して受信されたデータを保持する。計算用バッファは、ＣＰＵ２１が種々の計算をするため一時的な結果を保持する。送信用バッファは、通信部２５を通じてＩＣカード処理装置１に送信するデータを保持する。
- [0031] ＮＶＭ２４は、例えば、ＥＥＰＲＯＭあるいはフラッシュＲＯＭなどのデータの書き込み及び書換えが可能な不揮発性のメモリにより構成される。ＮＶＭ２４は、ＩＣカード２の運用用途に応じて制御プログラム、アプリケーション、及び種々のデータを格納する。例えば、ＮＶＭ２４では、プログラムファイル及びデータファイルなどが作成される。作成された各ファイルは、制御プログラム及び種々のデータなどが書き込まれる。なお、ＮＶＭ２４が、暗号情報及び識別情報を記憶してもよい。
- [0032] 通信部２５は、ＩＣカード処理装置１のカードリーダーライタ１４と通信し、所定の通信プロトコル等に応じたインタフェース（第１のインタフェース）により構成される。ＩＣカード２が接触型のＩＣカードとして実現される場合、通信部２５は、ＩＣカード処理装置１のカードリーダーライタ１４と物理的かつ電氣的に接触して信号の送受信を行うための通信制御部と接触部とにより構成される。また、ＩＣカード２が非接触型のＩＣカードとして実現

される場合、通信部 25 は、ＩＣカード処理装置 1 のカードリーダー 14 との無線通信を行うための変復調回路などの通信制御部とアンテナにより構成される。

[0033] また、ＩＣカード 2 が接触型及び非接触型の両方をサポートするデュアルカードである場合、通信部 25 は、ＩＣカード処理装置 1 のカードリーダー 14 と物理的かつ電氣的に接触して信号の送受信を行うための通信制御部と接触部、及びＩＣカード処理装置 1 のカードリーダー 14 との無線通信を行うための変復調回路などの通信制御部とアンテナにより構成される。

[0034] 以下、実施形態に係るセッション鍵共有処理について説明する。

実施形態に係るＩＣカード処理システムにおいて、ＩＣカード処理装置 1 は、ＩＣカード 2 から送信されるＰＱＣ暗号アルゴリズム及び鍵長に基づき、ＰＱＣの鍵ペアである公開鍵及び秘密鍵を、毎回、新規に生成し、公開鍵をＩＣカード 2 へ送信する。これにより、ＩＣカード 2 内に、固定の鍵を保管しておく必要がなくなり、不揮発性メモリの消費を抑えることが可能となる。ＩＣカード 2 は、乱数を生成し、受信した公開鍵に基づく暗号化処理により乱数から暗号化乱数を生成し、ＩＣカード処理装置 1 へ送信する。ＩＣカード 2 は、乱数からセッション鍵を生成し、また、ＩＣカード処理装置 1 は、秘密鍵に基づく復号処理により暗号化乱数から乱数を生成し、乱数からセッション鍵を生成し、ＩＣカード処理装置 1 及びＩＣカード 2 においてセッション鍵が共有される。

なお、ＩＣカード処理装置 1 は、公開鍵を生成するための情報をＩＣカード 2 へ送信し、ＩＣカード 2 は、受信した情報に基づいて公開鍵を生成してもよい。すなわち、ＩＣカード処理装置 1 は、必ずしも公開鍵そのものをＩＣカード 2 へ送信する方法に限らず、生成した公開鍵をＩＣカード 2 と共有できればよい。

[0035] ハードウェアリソースは、ＩＣカード 2 よりＩＣカード処理装置 1 の方が高いため、ＩＣカード処理装置 1 が、ＰＱＣの鍵ペアを生成する処理を担う

ことにより、情報処理システムとしてPQCに対応することができる。また、ICカード2は、PQCの鍵ペアを固定で保管する必要がなく、メモリへの負荷が軽減される。さらに、PQCの鍵ペアが、毎回、新規に生成されるため、秘密鍵が特定されるリスクを低減することができる。

[0036] 続いて、実施形態に係るセッション鍵共有処理について詳しく説明する。

＜概念1＞

図3は、実施形態に係るセッション鍵共有処理シーケンスの第1例を示す図である。ここで説明する第1例は、後に説明する第2例以降の上位の概念である。

ICカード処理装置1とICカード2の間で、セッション鍵による通信の暗号化を行うために、ICカード2のCPU21は、ROM22から暗号情報を読み出す。暗号情報は、ICカード2がサポートするPQC暗号アルゴリズム及び鍵長を含む。CPU21は、読み出した暗号情報をICカード処理装置1へ送信するよう制御し、通信部25は、暗号情報をICカード処理装置1へ送信する(ST101)。

[0037] ICカード処理装置1のカードリーダライタ14は、暗号情報を受信する。CPU11は、受信した暗号情報に含まれるPQC暗号アルゴリズム及び鍵長に基づき、公開鍵及び秘密鍵を生成する。即ち、CPU11は、受信した暗号情報に含まれるPQC暗号アルゴリズム及び鍵長のPQCの鍵ペアである公開鍵及び秘密鍵を生成する(ST102)。

[0038] CPU11は、公開鍵をICカード2へ送信するよう制御し、カードリーダライタ14は、公開鍵をICカード2へ送信する(ST103)。

[0039] 通信部25は、ICカード処理装置1から送信される公開鍵を受信し、CPU21は、受信された公開鍵を取得する。

[0040] CPU21は、乱数を生成し、取得した公開鍵に基づく暗号化処理により乱数から暗号化乱数を生成する。例えば、CPU21は、公開鍵に基づく暗号化処理により、乱数から暗号化乱数を生成する(ST104)。或いは、CPU21は、公開鍵に基づく暗号化処理により、乱数及び識別情報から暗

号化乱数を生成する。

[0041] CPU 21は、通信部25を介して暗号化乱数をICカード処理装置1へ送信するように制御し、通信部25は、暗号化乱数をICカード処理装置1へ送信する(ST105)。

[0042] CPU 21は、乱数に基づきセッション鍵を生成する(ST106)。CPU 21は、以降の処理で送信するデータをセッション鍵により暗号化し、通信部25は、セッション鍵により暗号化されたデータを送信する。

[0043] また、ICカード処理装置1のカードリーダー14は、暗号化乱数を受信する。CPU 11は、秘密鍵に基づく復号処理により暗号化乱数から乱数を生成する(ST107)。或いは、CPU 11は、秘密鍵に基づく復号処理により暗号化乱数から乱数及び識別情報を生成する。

[0044] CPU 11は、乱数に基づきセッション鍵を生成する(ST108)。CPU 11は、以降の処理で送信するデータをセッション鍵により暗号化し、カードリーダー14は、セッション鍵により暗号化されたデータを送信する。

[0045] 例えば、ICカード2は、ICカード処理装置1から受け取ったデータをセッション鍵で暗号化し、ICカード処理装置1へ暗号化データを送信する。ICカード処理装置1は、ICカード2から受け取ったデータをセッション鍵で暗号化し、ICカード2へ暗号化データを送信する。ICカード2及びICカード処理装置1は、受信した暗号化データに基づき、セッション鍵が正しく生成されたか否かを検証する。

[0046] 以上の処理により以下の作用効果が得られる。

PQCは複数方式が標準となり、ICカード2（例えばIC旅券）の発行元（例えば発行国）により異なる方式が搭載される可能性があるが、情報処理システムによれば、ICカード2から送信される暗号情報に含まれるPQC暗号アルゴリズム及び鍵長に基づき、IC旅券の方式の違いを吸収することができる。

[0047] また、情報処理システムによれば、公開鍵を使い捨て利用することにより

、固定鍵の長期間の運用には不安があったが、これを払拭することができる。

[0048] <概念 2 - 1>

図 4 は、実施形態に係るセッション鍵共有処理シーケンスの第 2 例を示す図である。なお、ここで説明する第 2 例は、先に説明した第 1 例の下位概念であり、相違部分を中心に説明し、共通部分の説明は適宜省略する。

[0049] IC カード処理装置 1 のオペレータは、OCR 15 の読み取り部を IC カード 2 の MR Z 20 へ翳す、又は IC カード 2 の MR Z 20 を OCR 15 の読み取り部へ翳す。これにより、OCR 15 は、IC カード 2 の MR Z 20 から識別情報を読み取る。CPU 11 は、読み取られた識別情報を取得する (ST 201)。図 4 では、MR Z 20 から読み取られる識別情報、及び ROM 22 から読み出される識別情報を MR Z と表記する。

[0050] IC カード 2 の CPU 21 は、ROM 22 から暗号情報を読み出し、読み出した暗号情報を IC カード処理装置 1 へ送信するよう制御し、通信部 25 は、暗号情報を IC カード処理装置 1 へ送信する (ST 202)。

[0051] IC カード処理装置 1 のカードリーダライタ 14 は、暗号情報を受信する。

[0052] CPU 21 は、第 1 の乱数 (RND) を生成し (ST 203)、ROM 22 から識別情報 (MR Z) を読み出し、第 1 の乱数を識別情報 (MR Z) により暗号化する (E (RND、MR Z))。つまり、CPU 21 は、読み出した識別情報 (MR Z) に基づく暗号化処理により第 1 の乱数から第 1 の暗号化乱数を生成する (ST 204)。

[0053] CPU 21 は、生成した第 1 の暗号化乱数 (Encrypted RND) を IC カード処理装置 1 へ送信するよう制御し、通信部 25 は、第 1 の暗号化乱数を IC カード処理装置 1 へ送信する (ST 205)。

[0054] カードリーダライタ 14 は、第 1 の暗号化乱数を受信する。

[0055] CPU 11 は、カードリーダライタ 14 を介して取得した第 1 の暗号化乱数を、OCR 15 を介して IC カード 2 から取得した識別情報 (MR Z) に

より復号する（D（RND、MRZ））。つまり、CPU11は、取得した識別情報（MRZ）に基づく復号処理により第1の暗号化乱数から第1の乱数を生成する（ST206）。

[0056] また、CPU11は、受信した暗号情報に含まれるPQC暗号アルゴリズム及び鍵長に基づき、公開鍵及び秘密鍵を生成する。即ち、CPU11は、受信した暗号情報に含まれるPQC暗号アルゴリズム及び鍵長のPQCの鍵ペアである公開鍵及び秘密鍵を生成する（ST207）。

[0057] CPU11は、公開鍵をICカード2へ送信するように制御し、カードリーダーライター14は、公開鍵をICカード2へ送信する（ST209）。

[0058] 通信部25は、ICカード処理装置1から送信される公開鍵を受信し、CPU21は、受信された公開鍵を取得する。

[0059] CPU21は、第2の乱数を生成し、取得した公開鍵に基づく暗号化処理により第2の乱数から第2の暗号化乱数を生成する（ST211）。

[0060] CPU21は、通信部25を介して第2の暗号化乱数をICカード処理装置1へ送信するように制御し、通信部25は、第2の暗号化乱数をICカード処理装置1へ送信する（ST212）。

[0061] また、CPU21は、第1及び第2の乱数に基づきセッション鍵を生成する（ST213）。CPU21は、以降の処理で送信するデータをセッション鍵により暗号化し、通信部25は、セッション鍵により暗号化されたデータを送信する。

[0062] また、CPU21は、第2の乱数に基づく暗号化処理によりMRZから暗号化MRZ（認証データ）を生成する（ST214）。

[0063] カードリーダーライター14は、第2の暗号化乱数を受信する。CPU11は、秘密鍵に基づく復号処理により第2の暗号化乱数から第2の乱数を生成する（ST215）。

[0064] CPU11は、第1及び第2の乱数に基づきセッション鍵を生成する（ST216）。CPU11は、以降の処理で送信するデータをセッション鍵により暗号化し、カードリーダーライター14は、セッション鍵により暗号化され

たデータを送信する。

[0065] また、CPU 21は、第2の乱数に基づく暗号化処理によりMRZから暗号化MRZ（認証データ）を生成する（ST217）。

[0066] 以上の処理により以下の作用効果が得られる。

情報処理システムによれば、OCR15を介して読み取られる識別情報と、カードリーダーライタ14を介して読み取られる暗号情報を併用することにより、どちらか一方の情報が安全であれば、最終的なセッション鍵を保護することができる。

[0067] また、情報処理システムによれば、公開鍵を使い捨てにすることで、仮に公開鍵への攻撃が発見されても、セッションが確立するまでの瞬時に公開鍵が解読されるようになるまでは、安全性を確保することができる。

[0068] <概念2-2>

図5は、実施形態に係るセッション鍵共有処理シーケンスの第3例を示す図である。なお、ここで説明する第3例は、先に説明した第2例の変形であり、相違部分を中心に説明し、共通部分の説明は適宜省略する。

[0069] 第2例で説明したように、ST201～ST207の処理が実行され、CPU11は、第1の乱数に基づく暗号化処理により、公開鍵から暗号化公開鍵（Encrypted Pub key）を生成する（ST208a）。例えば、CPU11は、AES（Advanced Encryption Standard）を利用し、第1の乱数を鍵として公開鍵を暗号化する。

[0070] CPU11は、暗号化公開鍵をICカード2へ送信するように制御し、カードリーダーライタ14は、公開鍵をICカード2へ送信する（ST209）。

[0071] 通信部25は、ICカード処理装置1から送信される暗号化公開鍵を受信し、CPU21は、受信された暗号化公開鍵を取得する。

[0072] CPU21は、第1の乱数に基づく復号処理により、暗号化公開鍵から公開鍵を生成する（ST210a）。例えば、CPU21は、AESを利用し、第1の乱数を鍵として暗号化公開鍵から公開鍵を取り出す。

[0073] CPU 21は、第2の乱数を生成し、取得した公開鍵に基づく暗号化処理により第2の乱数から第2の暗号化乱数を生成する（ST 211）。

[0074] CPU 21は、通信部 25 を介して第2の暗号化乱数を IC カード処理装置 1 へ送信するように制御し、通信部 25 は、第2の暗号化乱数を IC カード処理装置 1 へ送信する（ST 212）。

[0075] また、CPU 21は、第1及び第2の乱数に基づきセッション鍵を生成する（ST 213）。CPU 21は、以降の処理で送信するデータをセッション鍵により暗号化し、通信部 25 は、セッション鍵により暗号化されたデータを送信する。

[0076] また、CPU 21は、第2の乱数に基づく暗号化処理によりMRZから暗号化MRZ（認証データ）を生成する（ST 214）。

[0077] カードリーダーライタ 14 は、第2の暗号化乱数を受信する。CPU 11は、秘密鍵に基づく復号処理により第2の暗号化乱数から第2の乱数を生成する（ST 215）。

[0078] CPU 11は、第1及び第2の乱数に基づきセッション鍵を生成する（ST 216）。CPU 11は、以降の処理で送信するデータをセッション鍵により暗号化し、カードリーダーライタ 14 は、セッション鍵により暗号化されたデータを送信する。

[0079] また、CPU 21は、第2の乱数に基づく暗号化処理によりMRZから暗号化MRZ（認証データ）を生成する（ST 217）。

[0080] 以上の処理により以下の作用効果が得られる。

第1の暗号化乱数が解読されない限り、第三者は第1の乱数で暗号化される公開鍵を知り得ない。よって、情報処理システムによれば、解読するための糸口を与えず、安全性を高めることができる。

[0081] <概念 2-3>

図 6 は、実施形態に係るセッション鍵共有処理シーケンスの第 4 例を示す図である。なお、ここで第 4 例は、先に説明した第 3 例の変形であり、相違部分を中心に説明し、共通部分の説明は適宜省略する。

[0082] 第2例で説明したように、ST201～ST207の処理が実行され、CPU11は、MRZに基づく暗号化処理により、公開鍵から暗号化公開鍵を生成する(ST208b)。

[0083] CPU11は、暗号化公開鍵をICカード2へ送信するように制御し、カードリーダー14は、公開鍵をICカード2へ送信する(ST209)。

[0084] 通信部25は、ICカード処理装置1から送信される暗号化公開鍵を受信し、CPU21は、受信された暗号化公開鍵を取得する。

[0085] CPU21は、MRZに基づく復号処理により、暗号化公開鍵から公開鍵を生成する(ST210b)。

[0086] その後は、第2例で説明したようにST212～ST217の処理が実行される。

[0087] <概念3-1>

図7は、実施形態に係るセッション鍵共有処理シーケンスの第5例を示す図である。なお、ここで第5例は、先に説明した第2例～第4例の変形であり、相違部分を中心に説明し、共通部分の説明は適宜省略する。

[0088] 第5例では、PQC標準方式(Kyber)を利用する。図9は、PQC標準方式(Kyber)のAlgorithm 1の例示であり、図10は、PQC標準方式(Kyber)のAlgorithm 2の例示である。

[0089] PQCはデータ(公開鍵)サイズが大きいため、データ通信量及び計算時間が増大する。そこで、第5例では、公開鍵を生成する種情報を事前共有して通信量を削減し、また、ICカード処理装置1が事前計算を実行し公開鍵の一部を生成する。即ち、ICカード処理装置1の記憶部16は、公開鍵を生成する種情報であるPQC標準方式の一部又は全部を記憶し、ICカード2のROM22又はNVM24は、PQC標準方式の一部又は全部を記憶する。

[0090] 図7に示すように、ICカード処理装置1のオペレータは、OCR15の読み取り部をICカード2のMRZ20へ翳す、又はICカード2のMRZ

20をOCR15の読み取り部へ翳す。これにより、OCR15は、ICカード2のMRZ20から識別情報を読み取る。CPU11は、読み取られた識別情報を取得する(ST301)。図7では、MRZ20から読み取られる識別情報、及びROM22から読み出される識別情報をMRZと表記する。

- [0091] CPU21は、第1の乱数(RND)を生成し(ST302)、ROM22から識別情報(MRZ)を読み出し、第1の乱数を識別情報(MRZ)により暗号化する(E(RND、MRZ))。つまり、CPU21は、読み出した識別情報(MRZ)に基づく暗号化処理により第1の乱数から第1の暗号化乱数を生成する(ST303)。
- [0092] CPU21は、生成した第1の暗号化乱数をICカード処理装置1へ送信するよう制御し、通信部25は、第1の暗号化乱数をICカード処理装置1へ送信する(ST304)。
- [0093] カードリーダライタ14は、第1の暗号化乱数を受信する。
- [0094] CPU11は、カードリーダライタ14を介して取得した第1の暗号化乱数を、OCR15を介してICカード2から取得した識別情報(MRZ)により復号する(D(RND、MRZ))。つまり、CPU11は、取得した識別情報(MRZ)に基づく復号処理により第1の暗号化乱数から第1の乱数を生成する(ST305)。
- [0095] また、CPU11は、記憶部16に記憶されたPQC標準方式( $RND = \rho$  (Kyberの公開鍵の一部、かつ、行列Aの生成の源))に基づき、Kyberの鍵ペアである公開鍵( $p_k = (t, \rho)$ )及び秘密鍵( $s_k = s$ )を生成する(ST306)。
- [0096] CPU11は、平文のt(公開鍵の一部)を設定し(ST307)、tをICカード2へ送信するように制御し、カードリーダライタ14は、tをICカード2へ送信する(ST308)。又は、CPU11は、tを暗号化し(ST307)、暗号化されたtをICカード2へ送信するように制御し、カードリーダライタ14は、暗号化されたtをICカード2へ送信する(S

T 3 0 8)。

[0097] 通信部 2 5 は、I C カード処理装置 1 から送信される  $t$  又は暗号化された  $t$  を受信し、C P U 2 1 は、受信された  $t$  又は暗号化された  $t$  を取得する。

[0098] C P U 2 1 は、R O M 2 2 又は N V M 2 2 に記憶された P Q C 標準方式 (  $R N D = \rho$  (Kyberの公開鍵の一部、かつ、行列  $A$  の生成の源) ) に基づき、暗号化された  $t$  を取得した場合は暗号化された  $t$  から  $t$  を復号する (S T 3 0 9)。

[0099] また、C P U 2 1 は、第 2 の乱数を生成し、公開鍵に基づく暗号化処理により第 2 の乱数から第 2 の暗号化乱数を生成する (S T 3 1 0)。

[0100] C P U 2 1 は、通信部 2 5 を介して第 2 の暗号化乱数を I C カード処理装置 1 へ送信するように制御し、通信部 2 5 は、第 2 の暗号化乱数を I C カード処理装置 1 へ送信する (S T 3 1 1)。

[0101] また、C P U 2 1 は、第 1 及び第 2 の乱数に基づきセッション鍵を生成する (S T 3 1 2)。C P U 2 1 は、以降の処理で送信するデータをセッション鍵により暗号化し、通信部 2 5 は、セッション鍵により暗号化されたデータを送信する。

[0102] また、C P U 2 1 は、第 2 の乱数に基づく暗号化処理により M R Z から暗号化 M R Z (認証データ) を生成する (S T 3 1 3 A)。

[0103] カードリーダーライタ 1 4 は、第 2 の暗号化乱数を受信する。C P U 1 1 は、秘密鍵 ( $s k = s$ ) に基づく復号処理により第 2 の暗号化乱数から第 2 の乱数を生成する (S T 3 1 4)。

[0104] C P U 1 1 は、第 1 及び第 2 の乱数に基づきセッション鍵を生成する (S T 3 1 5)。C P U 1 1 は、以降の処理で送信するデータをセッション鍵により暗号化し、カードリーダーライタ 1 4 は、セッション鍵により暗号化されたデータを送信する。

[0105] また、C P U 2 1 は、第 2 の乱数に基づく暗号化処理により M R Z から暗号化 M R Z (認証データ) を生成する (S T 3 1 6 A)。

[0106] 以上の処理により以下の作用効果が得られる。

情報処理システムによれば、第1の暗号化乱数の導入時と同様に、第三者は公開鍵の一部である $\rho$ を知り得ない。よって、情報処理システムによれば、解読するための糸口を与えず、安全性を高めることができる。また、情報処理システムによれば、公開鍵の一部である $\rho$ を送受信する必要がないために、通信のデータサイズを削減できる。また、ICカード2は、第1の暗号化乱数( $RND = \rho$ )をリーダに送信後、待ち時間の間に $\rho$ を用いて先行的に暗号文を生成することができる。

[0107] <概念3-2>

図8は、実施形態に係るセッション鍵共有処理シーケンスの第6例を示す図である。なお、ここで第6例は、先に説明した第5例の変形であり、相違部分を中心に説明し、共通部分の説明は適宜省略する。

[0108] 第5例で説明したように、ST301~ST312、ST314、及びST315の処理が実行される。

[0109] 一方で、CPU21は、第2の乱数に基づく暗号化処理によりMRZから暗号化MRZ(第1の認証データ)を生成する(ST316B)。

[0110] カードリーダライタ14は、第1の認証データをICカード2へ送信する(ST317)。

[0111] また、CPU21は、第2の乱数に基づく暗号化処理により公開鍵から暗号化公開鍵(第2の認証データ)を生成する(ST313B)。

[0112] 通信部25は、第2の認証データをICカード処理装置1へ送信する(ST318)。

[0113] 上記説明した第1例~第5例に係る情報処理システムによれば、限られたハードウェアリソースにてPQCの搭載を可能とする携帯可能電子装置、情報処理装置、情報処理システム、及び情報処理方法を提供することができる。

[0114] 公開鍵に関するバリエーションとしては、以下が挙げられる。

(1) ICカード処理装置1は、公開鍵を平文で送信する。

(2) ICカード処理装置1は、公開鍵を第1の乱数で暗号化して、暗号化

された公開鍵を送信する。

(3) ICカード処理装置1は、公開鍵をMRZ20から読み取られた識別情報で暗号化して、暗号化された公開鍵を送信する。

(4) ICカード処理装置1は、 $p$ を生成し、 $p$ から $t$ を生成し、 $t$ を平文で送信する。(5) ICカード処理装置1は、 $p$ を生成し、 $p$ から $t$ を生成し、 $t$ を暗号化し、暗号化された $t$ を送信する。

(6) ICカード2は、 $p$ と第1の乱数を生成し、 $p$ と第1の乱数の両方を送信する。ICカード処理装置1は、 $p$ から $t$ を生成する。

(7) ICカード2は、 $p$ を生成し、 $p$ を第1の乱数とし、 $p$ を送信する。ICカード処理装置1は、 $p$ から $t$ を生成する。

(8) ICカード2は、第1の乱数そのものを $p$ にするのではなく、第1の乱数をハッシュして $p$ にする。

(9) ICカード処理装置1及びICカード2は、第2の乱数をセッションキーとする。(10) ICカード処理装置1及びICカード2は、第1の乱数と第2の乱数の排他的論理和(XOR)からセッションキーを生成する。

[0115] セッションキー確認手段のバリエーションとしては、以下が挙げられる。

(1) ICカード処理装置1及びICカード2は、MRZ20から読み取られた識別情報を第2の乱数で暗号化した認証データを交換して、セッションキーを検証する。

(2) ICカード処理装置1及びICカード2は、MRZ20から読み取られた識別情報を第1の乱数と第2の乱数に対して排他的論理和を行った結果で暗号化して、セッションキーを検証する。

[0116] 暗号アルゴリズムと鍵長の提示バリエーションとしては、以下が挙げられる。

(1) ICカード2は、MRZ20と併せて、暗号アルゴリズムと鍵長を含む暗号情報を提示する。例えば、ICカード処理装置1のOCR15によりMRZ20を光学的に読み取らせ、ICカード処理装置1のカードリーダー14により暗号情報を受信させる。(2) ICカード2は、第1の乱数

と併せて、暗号アルゴリズムと鍵長を含む暗号情報を提示する。例えば、ＩＣカード２は、第１の乱数及び暗号情報を含む情報を暗号化して提示する。

(３) ＩＣカード２は、第１の乱数とは別に、暗号アルゴリズムと鍵長を含む暗号情報を平文で提示する。

[0117] また、上記説明では、ＩＣカード処理装置１は、ＯＣＲ１５を介して識別情報を取得するケースについて説明したが、これに限定されるものではない。例えば、ＩＣカード２の通信部２５が、ＲＯＭ２２等に記憶される識別情報を送信し、ＩＣカード処理装置１のカードリーダー１４が、ＩＣカード２から送信される識別情報を受信するようにしてもよい。その場合、ＩＣカード２のＣＰＵ２１は、異なる通信方式（接触通信と非接触通信）を用いて、暗号化された乱数及び平文又は暗号化された鍵の送受信と、識別情報の送信とを実現するようにしてもよい。

[0118] 例えば、ＩＣカード２の通信部２５は、接触通信（物理的かつ電氣的に接触して信号の送受信を行うための通信制御部と接触部）により、暗号化された乱数及び平文又は暗号化された鍵を送受信し、また、非接触通信（無線通信を行うための変復調回路などの通信制御部とアンテナ）により、識別情報を送信する。一方のＩＣカード処理装置１のカードリーダー１４は、接触通信により、暗号化された乱数及び平文又は暗号化された鍵を送受信し、また、非接触通信により、識別情報を受信する。

[0119] 或いは、ＩＣカード２の通信部２５は、接触通信により、識別情報を送信し、また、非接触通信により、暗号化された乱数及び平文又は暗号化された鍵を送受信する。一方のＩＣカード処理装置１のカードリーダー１４は、接触通信により、識別情報を受信し、また、非接触通信により、暗号化された乱数及び平文又は暗号化された鍵を送受信する。

[0120] 上記の通り、実施形態に係る情報処理システムは、乱数及び鍵の送受信と、識別情報の送受信とを異なる通信方式で実現する。これにより、乱数及び鍵と、識別情報とが同時に盗まれるリスクを大幅に低減することができ、セキュリティの向上を図ることができる。

[0121] なお、本実施形態に係るプログラムは、ＩＣカード処理装置１及びＩＣカード２等の電子機器に記憶された状態で譲渡されてよいし、電子機器に記憶されていない状態で譲渡されてもよい。後者の場合は、プログラムは、ネットワークを介して譲渡されてよいし、記憶媒体に記憶された状態で譲渡されてもよい。記憶媒体は、非一時的な有形の媒体である。記憶媒体は、コンピュータ可読媒体である。記憶媒体は、光ディスク、メモリカード等のプログラムを記憶可能かつコンピュータで読取可能な媒体であればよく、その形態は問わない。電子機器は、ネットワークを介して譲渡（提供）されるプログラムをダウンロードしてメモリにインストールする、又は記憶媒体からプログラムを読み取りメモリにインストールする。

[0122] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

### 請求の範囲

- [請求項1]           暗号アルゴリズムを含む暗号情報を記憶するメモリと、  
                      情報処理装置と通信するインタフェースと、  
                      乱数を生成するプロセッサと、を備え、  
                      前記インタフェースは、前記暗号情報を前記情報処理装置へ送信し、  
                      前記暗号アルゴリズムに基づき生成される公開鍵及び秘密鍵のうちの  
                      前記情報処理装置から送信される前記公開鍵を受信し、  
                      前記プロセッサは、前記公開鍵に基づく暗号化処理により前記乱数  
                      から暗号化乱数を生成し、  
                      前記インタフェースは、前記暗号化乱数を前記情報処理装置へ送信  
                      し、  
                      前記プロセッサは、前記乱数に基づき前記情報処理装置との通信に  
                      使用するセッション鍵を生成する、携帯可能電子装置。
- [請求項2]           前記暗号アルゴリズムは、耐量子計算機暗号を用いた暗号アルゴリ  
                      ズムである、  
                      請求項1に記載の携帯可能電子装置。
- [請求項3]           前記情報処理装置において、前記秘密鍵に基づく復号処理により前  
                      記暗号化乱数から前記乱数を生成させ、前記乱数に基づき前記携帯可  
                      能電子装置との通信に使用する前記セッション鍵を生成させるために  
                      、前記インタフェースは、前記暗号化乱数を前記情報処理装置へ送信  
                      する、請求項1の携帯可能電子装置。
- [請求項4]           前記暗号情報は、鍵長を含み、  
                      前記公開鍵及び前記秘密鍵は、前記暗号情報に含まれる前記暗号ア  
                      ルゴリズム及び前記鍵長に基づき生成される、請求項1の携帯可能電  
                      子装置。
- [請求項5]           前記メモリは、当該携帯可能電子装置を識別可能な識別情報を記憶  
                      し、  
                      前記プロセッサは、第1の乱数を生成し、前記識別情報に基づく暗

号化处理により前記第 1 の乱数から第 1 の暗号化乱数を生成し、

前記インタフェースは、前記第 1 の暗号化乱数を前記情報処理装置へ送信し、前記情報処理装置から送信される前記公開鍵を受信し、

前記プロセッサは、第 2 の乱数を生成し、前記公開鍵に基づく暗号化处理により前記第 2 の乱数から第 2 の暗号化乱数を生成し、

前記インタフェースは、前記第 2 の暗号化乱数を前記情報処理装置へ送信し、

前記プロセッサは、前記第 1 及び第 2 の乱数に基づき前記セッション鍵を生成する、請求項 1 の携帯可能電子装置。

[請求項 6] 前記情報処理装置において、当該携帯可能電子装置から取得した前記識別情報に基づく復号処理により前記第 1 の暗号化乱数から前記第 1 の乱数を生成させ、前記秘密鍵に基づく復号処理により前記第 2 の暗号化乱数から前記第 2 の乱数を生成させ、前記第 1 及び第 2 の乱数に基づき前記セッション鍵を生成させるために、前記インタフェースは、前記第 1 及び第 2 の暗号化乱数を前記情報処理装置へ送信する、請求項 5 の携帯可能電子装置。

[請求項 7] 前記情報処理装置は、前記第 1 の乱数に基づく暗号化处理により前記公開鍵から暗号化公開鍵を生成し、前記公開鍵に替えて前記暗号化公開鍵を送信し、  
前記インタフェースは、前記情報処理装置から送信される前記暗号化公開鍵を受信し、前記プロセッサは、前記第 1 の乱数に基づく復号処理により前記暗号化公開鍵から前記公開鍵を生成する、請求項 5 の携帯可能電子装置。

[請求項 8] 前記識別情報が印刷されたリーダブルゾーンを備え、  
前記情報処理装置は、前記リーダブルゾーンから光学的に読み取り可能な外部インタフェースを介して前記識別情報を取得し、前記識別情報に基づく復号処理により前記第 1 の暗号化乱数から前記第 1 の乱数を生成する、請求項 5 の携帯可能電子装置。

- [請求項9] 前記インタフェースは、所定の通信プロトコルに基づき接触又は非接触により前記情報処理装置と通信するインタフェースであって、  
前記プロセッサは、前記インタフェースを介して前記情報処理装置へ前記識別情報を送信し、  
前記情報処理装置は、前記識別情報を前記インタフェースを介して取得し、前記識別情報に基づく復号処理により前記第1の暗号化乱数から前記第1の乱数を生成する、請求項5の携帯可能電子装置。
- [請求項10] 前記インタフェースは、  
接触通信により、前記識別情報を前記情報処理装置へ送信し、  
非接触通信により、前記第1の暗号化乱数を前記情報処理装置へ送信し、前記情報処理装置から送信される前記公開鍵を受信し、前記第2の暗号化乱数を前記情報処理装置へ送信する、  
又は、前記非接触通信により、前記識別情報を前記情報処理装置へ送信し、  
前記接触通信により、前記第1の暗号化乱数を前記情報処理装置へ送信し、前記情報処理装置から送信される前記公開鍵を受信し、前記第2の暗号化乱数を前記情報処理装置へ送信する、請求項9の携帯可能電子装置。
- [請求項11] 携帯可能電子装置と通信するインタフェースと、  
鍵を生成するプロセッサと、を備え、  
前記インタフェースは、前記携帯可能電子装置から送信される暗号情報を受信し、  
前記プロセッサは、前記暗号情報に含まれる暗号アルゴリズムに基づき公開鍵及び秘密鍵を生成し、  
前記インタフェースは、前記公開鍵を前記携帯可能電子装置へ送信し、前記携帯可能電子装置において前記公開鍵に基づく暗号化処理により乱数から生成される暗号化乱数を受信し、  
前記プロセッサは、前記秘密鍵に基づく復号処理により前記暗号化

乱数から前記乱数を生成し、前記乱数に基づき前記携帯可能電子装置との通信に使用するセッション鍵を生成する、情報処理装置。

[請求項12] 携帯可能電子装置及び情報処理装置を備える情報処理システムであって、

前記携帯可能電子装置は、

暗号アルゴリズムを含む暗号情報を記憶するメモリと、

前記情報処理装置と通信する第1のインタフェースと、

乱数を生成するプロセッサと、を備え、

前記第1のインタフェースは、前記暗号情報を前記情報処理装置へ送信し、前記暗号アルゴリズムに基づき生成される公開鍵及び秘密鍵のうちの前記情報処理装置から送信される前記公開鍵を受信し、

前記プロセッサは、前記公開鍵に基づく暗号化処理により前記乱数から暗号化乱数を生成し、

前記第1のインタフェースは、前記暗号化乱数を前記情報処理装置へ送信し、

前記プロセッサは、前記乱数に基づき前記情報処理装置との通信に使用するセッション鍵を生成し、

前記情報処理装置は、

前記携帯可能電子装置と通信する第2のインタフェースと、

鍵を生成する第2のプロセッサと、を備え、

前記第2のインタフェースは、前記携帯可能電子装置から送信される前記暗号情報を受信し、

前記第2のプロセッサは、前記暗号情報に含まれる前記暗号アルゴリズムに基づき前記公開鍵及び前記秘密鍵を生成し、

前記第2のインタフェースは、前記公開鍵を前記携帯可能電子装置へ送信し、前記携帯可能電子装置において前記公開鍵に基づく暗号化処理により前記乱数から生成される前記暗号化乱数を受信し、

前記第2のプロセッサは、前記秘密鍵に基づく復号処理により前

記暗号化乱数から前記乱数を生成し、前記乱数に基づき前記携帯可能電子装置との通信に使用する前記セッション鍵を生成する、情報処理システム。

[請求項13] 携帯可能電子装置及び情報処理装置により実行される情報処理方法であって、

前記携帯可能電子装置は、暗号アルゴリズムを含む暗号情報を前記情報処理装置へ送信し、

前記情報処理装置は、前記携帯可能電子装置から送信される前記暗号情報を受信し、前記暗号情報に含まれる前記暗号アルゴリズムに基づき公開鍵及び秘密鍵を生成し、前記公開鍵を前記携帯可能電子装置へ送信し、

前記携帯可能電子装置は、前記情報処理装置から送信される前記公開鍵を受信し、前記公開鍵に基づく暗号化処理により乱数から暗号化乱数を生成し、前記暗号化乱数を前記情報処理装置へ送信し、前記乱数に基づき前記情報処理装置との通信に使用するセッション鍵を生成し、

前記情報処理装置は、前記携帯可能電子装置から送信される前記暗号化乱数を受信し、前記秘密鍵に基づく復号処理により前記暗号化乱数から前記乱数を生成し、前記乱数に基づき前記携帯可能電子装置との通信に使用する前記セッション鍵を生成する、情報処理方法。