(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2010-4226
(P2010-4226A)
(43)公開日　平成22年1月7日(2010.1.7)

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

審査請求 未請求　請求項の数 14　ＯＬ　（全 15 頁）

(21)出願番号　特願2008-160201 (P2008-160201)
(22)出願日　平成20年6月19日 (2008.6.19)

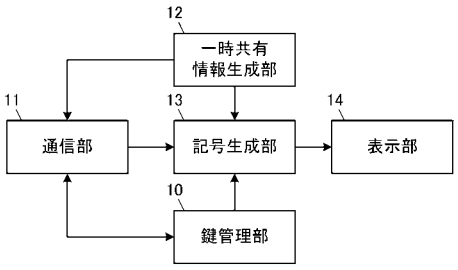
特許法第３０条第１項適用申請有り　平成２０年２月２０日　国立大学法人九州大学主催の「卒業論文試問」に発表

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(71)出願人　504145342
国立大学法人九州大学
福岡県福岡市東区箱崎六丁目１０番１号
(74)代理人　100072604
弁理士　有我　軍一郎
(72)発明者　北口　貴史
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　津村　直樹
東京都大田区中馬込１丁目３番６号　株式会社リコー内

最終頁に続く

(54)【発明の名称】情報通信装置および公開鍵認証方法

(57)【要約】
【課題】認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる情報通信装置および公開鍵認証方法を提供すること。
【解決手段】自己の公開鍵と相手の公開鍵とを交換する通信部１１と、自己の公開鍵と相手の公開鍵と一時的な共有情報とに基づいた記号を生成する記号生成部１３と、記号生成部１３で生成された記号に応じた情報を表示する表示部１４とを備え、表示部１４に表示された情報が自己と相手とで同一のものであるか否かを各ユーザに視認させることで、自己の公開鍵と相手の公開鍵とを相互に認証させる。
【選択図】図２



【特許請求の範囲】
【請求項１】
自己の公開鍵と相手の公開鍵とを交換する通信部と、
前記自己の公開鍵と前記相手の公開鍵と一時的な共有情報とに基づいた記号を生成する記号生成部と、
前記記号生成部で生成された記号に応じた情報を表示する表示部と、
前記表示部に表示された情報が自己と相手とで同一のものであるか否かを表す認証情報を受付ける認証情報受付部と、を備え、
前記認証情報受付部に受付けられた認証情報に基づいて、前記自己の公開鍵と前記相手の公開鍵とを前記相手側との間で相互に認証する情報通信装置。
【請求項２】
乱数を発生する乱数発生部を備え、
前記通信部が、前記乱数発生部と相手側の乱数発生部とによってそれぞれ発生された乱数を交換し、
前記記号生成部が、前記通信部によって交換された乱数を前記一時的な共有情報として前記記号を生成することを特徴とする請求項１に記載の情報通信装置。
【請求項３】
乱数を発生する乱数発生部を備え、
前記通信部が、前記乱数発生部によって発生された乱数を相手側に送信し、
前記記号生成部が、前記乱数発生部によって発生された乱数を前記一時的な共有情報として前記記号を生成することを特徴とする請求項１に記載の情報通信装置。
【請求項４】
前記通信部が、相手側から送信された乱数を受信し、
前記記号生成部が、前記通信部によって受信された乱数を前記一時的な共有情報として前記記号を生成することを特徴とする請求項１に記載の情報通信装置。
【請求項５】
自己と相手との間で一時的に取り決められたパスワードが入力される入力部を備え、
前記記号生成部が、該パスワードを前記一時的な共有情報として前記記号を生成することを特徴とする請求項１に記載の情報通信装置。
【請求項６】
前記記号発生部が、前記自己の公開鍵と前記相手の公開鍵と前記一時的な共有情報とを結合した情報のハッシュ値を前記記号として算出することを特徴とする請求項１乃至請求項５の何れかに記載の情報通信装置。
【請求項７】
前記記号生成部が、前記記号の少なくとも一部に基づいて文字列を生成し、
前記表示部が、前記文字列を表示することを特徴とする請求項１乃至請求項６の何れかに記載の情報通信装置。
【請求項８】
前記記号生成部が、前記記号の少なくとも一部を複数の記号に分割し、分割した各記号を一意に表す文字列に変換し、
前記表示部が、前記各文字列を表示することを特徴とする請求項１乃至請求項６の何れかに記載の情報通信装置。
【請求項９】
第１の情報通信装置のユーザと第２の情報通信装置のユーザとの間で、公開鍵を相互に認証させる公開鍵認証方法において、
前記第１および第２の情報通信装置が、双方のユーザの公開鍵を交換する通信ステップと、
前記第１および第２の情報通信装置が、前記双方のユーザの公開鍵と一時的な共有情報とに基づいた記号をそれぞれ生成する記号生成ステップと、
前記第１および第２の情報通信装置が、前記記号生成ステップでそれぞれ生成した記号

に応じた情報をそれぞれ表示する表示ステップと、
前記第１および第２の情報通信装置が、前記表示ステップで表示された情報が相互に同一のものであるか否かを表す認証情報を受付ける受付ステップと、
前記第１および第２の情報通信装置が、前記受付ステップで受付けた認証情報に基づいて、前記双方の公開鍵を相互に認証する認証ステップと、を有することを特徴とする公開鍵認証方法。
【請求項１０】
前記第１および第２の情報通信装置の少なくとも一方が、乱数を発生する乱数発生ステップを有し、
前記通信ステップで、前記第１および第２の情報通信装置が、前記乱数を送受信し、
前記記号生成ステップで、前記第１および第２の情報通信装置が、前記乱数を前記一時的な共有情報として前記記号をそれぞれ生成することを特徴とする請求項９に記載の公開鍵認証方法。
【請求項１１】
前記第１および第２の情報通信装置が、一時的に相互に取り決められたパスワードをそれぞれ入力させる入力ステップを有し、
前記記号生成ステップで、前記第１および第２の情報通信装置が、前記パスワードを前記一時的な共有情報として前記記号をそれぞれ生成することを特徴とする請求項９に記載の公開鍵認証方法。
【請求項１２】
前記記号生成ステップで、前記第１および第２の情報通信装置が、前記双方の公開鍵と前記一時的な共有情報とを結合した情報のハッシュ値を前記記号としてそれぞれ生成することを特徴とする請求項９乃至請求項１１の何れかに記載の公開鍵認証方法。
【請求項１３】
前記記号生成ステップで、前記第１および第２の情報通信装置が、前記記号の少なくとも一部に基づいて文字列をそれぞれ生成し、
前記表示ステップで、前記第１および第２の情報通信装置が、前記文字列をそれぞれ表示することを特徴とする請求項９乃至請求項１２の何れかに記載の公開鍵認証方法。
【請求項１４】
前記記号生成ステップで、前記第１および第２の情報通信装置が、前記記号の少なくとも一部を複数の記号にそれぞれ分割し、分割した各記号を一意に表す文字列にそれぞれ変換し、
前記表示ステップで、前記第１および第２の情報通信装置が、前記文字列をそれぞれ表示することを特徴とする請求項９乃至請求項１２の何れかに記載の公開鍵認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報通信装置および公開鍵認証方法に関し、特に、認証局が存在しない通信環境で公開鍵を認証する情報通信装置および公開鍵認証方法に関する。
【背景技術】
【０００２】
近年、携帯電話やガジェットなどの携帯端末の普及に伴い、ユーザ同士が携帯端末を持ち寄り、無線ＬＡＮ（Local Area Network）やＢｌｕｅｔｏｏｔｈ（登録商標）等のような規格に準拠した無線通信によって、名刺交換、電子マネーの譲渡および会議等の情報交換を行うことができるようになってきている。
【０００３】
このような無線通信において、悪意のあるユーザによる通信内容の盗聴や改ざんを防止するためには、通信内容を暗号化する必要がある。通信内容を暗号化するために、公開鍵暗号方式を用いて暗号化に用いる鍵をユーザ間で安全に共有する技術がある。
【０００４】

公開鍵暗号方式では、公開鍵を使用する前に、その公開鍵が本人のものであるか否かを認証する必要がある。インターネット網に接続できる環境においては、認証局を利用して公開鍵を認証することができるが、上述した無線通信のように認証局が存在しない通信環境においては、認証局を利用することができない。

【０００５】

このような通信環境において、公開鍵を認証させるものとして、Biometric Word Listsといった英単語の表を用い、公開鍵のハッシュ値を１バイト毎に英単語に変換して口頭で読み上げることによって、公開鍵の送り手と受け手でハッシュ値の一致性を確認するものがある（例えば、非特許文献１、２参照）。

【非特許文献１】P. Zimmermann、「PGPfone Owner's Manual」、１９９６年７月

【非特許文献２】P. Juola and P. Zimmermann、「Whole-word phonetic distances and PGPfone alphabet」、Proceeding of Fourth international Conference on Spoken Language Processing，Ｖｏｌ．１，ｐｐ．９８－１０１、１９９６年１０月

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、上述した従来の技術においては、ユーザ同士が相互に公開鍵の認証を行う場合に、膨大な英単語を誤ることなく双方向に照合する必要があり、ユーザにかかる負担が大きいといった課題があった。

【０００７】

本発明は、従来の課題を解決するためになされたもので、認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる情報通信装置および公開鍵認証方法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】

【０００８】

本発明の情報通信装置は、自己の公開鍵と相手の公開鍵とを交換する通信部と、前記自己の公開鍵と前記相手の公開鍵と一時的な共有情報とに基づいた記号を生成する記号生成部と、前記記号生成部で生成された記号に応じた情報を表示する表示部と、前記表示部に表示された情報が自己と相手とで同一のものであるか否かを表す認証情報を受付ける認証情報受付部と、を備え、前記認証情報受付部に受付けられた認証情報に基づいて、前記自己の公開鍵と前記相手の公開鍵とを前記相手側との間で相互に認証する構成を有している。

【０００９】

この構成により、本発明の情報通信装置は、表示部に表示された情報が自己と相手とで同一のものであるか否かを視認させることで、自己の公開鍵と相手の公開鍵とを相互に認証させるため、認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる。

【００１０】

なお、本発明の情報通信装置は、乱数を発生する乱数発生部を備え、前記通信部が、前記乱数発生部と相手側の乱数発生部とによってそれぞれ発生された乱数を交換し、前記記号生成部が、前記通信部によって交換された乱数を前記一時的な共有情報として前記記号を生成するようにしてもよい。

【００１１】

この構成により、本発明の情報通信装置は、公開鍵を相互に認証する時に自己と相手側とでそれぞれ発生した乱数を含む情報に基づいた記号を生成するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００１２】

また、本発明の情報通信装置は、乱数を発生する乱数発生部を備え、前記通信部が、前記乱数発生部によって発生された乱数を相手側に送信し、前記記号生成部が、前記乱数発

生部によって発生された乱数を前記一時的な共有情報として前記記号を生成するようにしてもよい。

【００１３】

この構成により、本発明の情報通信装置は、公開鍵を相互に認証する時に自己で発生した乱数を含む情報に基づいた記号を生成するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００１４】

また、前記通信部が、相手側から送信された乱数を受信し、前記記号生成部が、前記通信部によって受信された乱数を前記一時的な共有情報として前記記号を生成するようにしてもよい。

【００１５】

この構成により、本発明の情報通信装置は、公開鍵を相互に認証する時に相手側で発生された乱数を含む情報に基づいた記号を生成するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００１６】

また、本発明の情報通信装置は、自己と相手との間で一時的に取り決められたパスワードが入力される入力部を備え、前記記号生成部が、該パスワードを前記一時的な共有情報として前記記号を生成するようにしてもよい。

【００１７】

この構成により、本発明の情報通信装置は、自己と相手との間で一時的に取り決められたパスワードを含む情報に基づいた記号を生成するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００１８】

また、前記記号発生部が、前記自己の公開鍵と前記相手の公開鍵と前記一時的な共有情報とを結合した情報のハッシュ値を前記記号として算出するようにしてもよい。

【００１９】

この構成により、本発明の情報通信装置は、双方の公開鍵と一時的な共有情報とを結合した情報のハッシュ値を認証時の記号として算出するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００２０】

ここで、前記記号生成部が、前記記号の少なくとも一部に基づいて文字列を生成し、前記表示部が、前記文字列を表示するようにしてもよい。

【００２１】

この構成により、本発明の情報通信装置は、照合に用いる文字列の数を削減することができるため、文字列を照合するときに照合誤りが発生することを防止することができる。

【００２２】

また、前記記号生成部が、前記記号の少なくとも一部を複数の記号に分割し、分割した各記号を一意に表す文字列に変換し、前記表示部が、前記各文字列を表示するようにしてもよい。

【００２３】

この構成により、本発明の情報通信装置は、照合に用いる文字列の数を削減することができるため、文字列を照合するときに照合誤りが発生することを防止することができる。

【００２４】

本発明の公開鍵認証方法は、第１の情報通信装置のユーザと第２の情報通信装置のユーザとの間で、公開鍵を相互に認証させる公開鍵認証方法において、前記第１および第２の情報通信装置が、双方のユーザの公開鍵を交換する通信ステップと、前記第１および第２

の情報通信装置が、前記双方のユーザの公開鍵と一時的な共有情報とに基づいた記号をそれぞれ生成する記号生成ステップと、前記第１および第２の情報通信装置が、前記記号生成ステップでそれぞれ生成した記号に応じた情報をそれぞれ表示する表示ステップと、前記第１および第２の情報通信装置が、前記表示ステップで表示された情報が相互に同一のものであるか否かを表す認証情報を受付ける受付ステップと、前記第１および第２の情報通信装置が、前記受付ステップで受付けた認証情報に基づいて、前記双方の公開鍵を相互に認証する認証ステップと、を有する。

【００２５】

したがって、本発明の公開鍵認証方法は、表示ステップで表示された情報が第１の情報通信装置と第２の情報通信装置とで同一のものであるか否かを視認させることで、第１および第２の情報通信装置のユーザの公開鍵を相互に認証させるため、認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる。

【００２６】

また、本発明の公開鍵認証方法は、前記第１および第２の情報通信装置の少なくとも一方が、乱数を発生する乱数発生ステップを有し、前記通信ステップで、前記第１および第２の情報通信装置が、前記乱数を送受信し、前記記号生成ステップで、前記第１および第２の情報通信装置が、前記乱数を前記一時的な共有情報として前記記号をそれぞれ生成するようにしてもよい。

【００２７】

したがって、本発明の公開鍵認証方法は、公開鍵を相互に認証する時に第１および第２の情報通信装置の少なくとも一方で発生した乱数を含む情報に基づいた記号を生成するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００２８】

また、本発明の公開鍵認証方法は、前記第１および第２の情報通信装置が、一時的に相互に取り決められたパスワードをそれぞれ入力させる入力ステップを有し、前記記号生成ステップで、前記第１および第２の情報通信装置が、前記パスワードを前記一時的な共有情報として前記記号をそれぞれ生成するようにしてもよい。

【００２９】

したがって、本発明の公開鍵認証方法は、前記第１および第２の情報通信装置のユーザの間で一時的に取り決められたパスワードを含む情報に基づいた記号を生成するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００３０】

また、本発明の公開鍵認証方法は、前記記号生成ステップで、前記第１および第２の情報通信装置が、前記双方の公開鍵と前記一時的な共有情報とを結合した情報のハッシュ値を前記記号としてそれぞれ生成するようにしてもよい。

【００３１】

したがって、本発明の公開鍵認証方法は、双方の公開鍵と一時的な共有情報とを結合した情報のハッシュ値を認証時の記号として算出するため、悪意のあるユーザが、同一の記号を生成させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることを防止することができる。

【００３２】

また、本発明の公開鍵認証方法は、前記記号生成ステップで、前記第１および第２の情報通信装置が、前記記号の少なくとも一部に基づいて文字列をそれぞれ生成し、前記表示ステップで、前記第１および第２の情報通信装置が、前記文字列をそれぞれ表示するようにしてもよい。

【００３３】

したがって、本発明の公開鍵認証方法は、照合に用いる文字列の数を削減することがで

きるため、文字列を照合するときに照合誤りが発生することを防止することができる。
【００３４】
また、本発明の公開鍵認証方法は、前記記号生成ステップで、前記第１および第２の情報通信装置が、前記記号の少なくとも一部を複数の記号にそれぞれ分割し、分割した各記号を一意に表す文字列にそれぞれ変換し、前記表示ステップで、前記第１および第２の情報通信装置が、前記文字列をそれぞれ表示するようにしてもよい。
【００３５】
したがって、本発明の公開鍵認証方法は、照合に用いる文字列の数を削減することができるため、文字列を照合するときに照合誤りが発生することを防止することができる。
【発明の効果】
【００３６】
本発明は、認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる情報通信装置および公開鍵認証方法を提供することができる。
【発明を実施するための最良の形態】
【００３７】
以下、本発明の実施の形態について、図面を参照して説明する。なお、本実施の形態においては、本発明の情報通信装置を図１に示すような構成を有する携帯端末によって実現した例について説明する。
【００３８】
図１に示すように、本実施の形態に係る携帯端末は、ＣＰＵ（Central Processing Unit）１と、ＲＡＭ（Random Access Memory）２と、ＲＯＭ（Read Only Memory）３と、ハードディスク装置やフラッシュメモリ等の不揮発性の記憶媒体（本実施の形態においては、フラッシュメモリとする）４と、キーボード装置やポインティングデバイスからなる入力装置５と、液晶ディスプレイ等よりなる表示装置６と、無線ＬＡＮ、ＢｌｕｅｔｏｏｔｈまたはＺｉｇＢｅｅ（登録商標）等の無線通信規格に準拠した通信を行う無線通信モジュール７とを備えている。
【００３９】
ＲＯＭ３およびフラッシュメモリ４には、当該携帯端末を本発明の情報通信装置として機能させるためにＣＰＵ１に実行させるプログラムが格納されている。例えば、ＲＡＭ２を一時記憶領域として当該プログラムを実行するＣＰＵ１は、当該携帯端末のユーザの秘密鍵および公開鍵からなる鍵ペアを生成し、生成した鍵ペアをフラッシュメモリ４に格納するようになっている。
【００４０】
また、ＣＰＵ１は、認証済みの他者の公開鍵をフラッシュメモリ４に格納しておき、自己の公開鍵と、認証済みの相手の公開鍵とに基づいて、共有秘密鍵を生成し、生成した共有秘密鍵で無線通信モジュール７を介して送受信する情報の暗号化および復号を行うようになっている。
【００４１】
図２は、前述した携帯端末における公開鍵認証にかかる機能を説明するための機能ブロック図である。図２において、携帯端末は、自己の鍵ペアおよび認証済みの他者の公開鍵を管理する鍵管理部１０と、自己の公開鍵と相手の公開鍵とを交換する通信部１１と、一時的な共有情報を生成する一時共有情報生成部１２と、自己の公開鍵と相手の公開鍵と一時的な共有情報とに基づいた記号を生成する記号生成部１３と、記号生成部１３で生成された記号に応じた情報を表示する表示部１４とを備えている。
【００４２】
ここで、鍵管理部１０は、ＣＰＵ１およびフラッシュメモリ４によって構成され、通信部１１は、ＣＰＵ１および無線通信モジュール７によって構成される。また、一時共有情報生成部１２および記号生成部１３は、ＣＰＵ１によって構成され、表示部１４は、ＣＰＵ１および表示装置６によって構成される。

【００４３】
以上のように構成された携帯端末のより詳細な実施の形態について、以下に説明する。
【００４４】
（第１の実施の形態）
本発明の第１の実施の形態としての携帯端末において、一時共有情報生成部１２は、一時的な共有情報として乱数を生成する乱数発生部によって構成される。通信部１１は、公開鍵に加えて、一時共有情報生成部１２によって生成された乱数を相手の携帯端末と交換するようになっている。
【００４５】
記号生成部１３は、ホストの公開鍵と、ホストの携帯端末の一時共有情報生成部１２によって生成された乱数（以下、単に「ホストの乱数」という。）と、ゲストの公開鍵と、ゲストの携帯端末の一時共有情報生成部１２によって生成された乱数（以下、単に「ゲストの乱数」という。）とを結合した結合情報に対して、ＳＨＡ－１（Secure Hash Algorithm 1）等の一方向性関数を用いてハッシュ値を算出するようになっている。
【００４６】
ここで、ホストとは、相互の公開鍵認証（以下、「公開鍵相互認証」という。）を要求した携帯端末のユーザのことをいい、ゲストとは、この要求に応じた携帯端末のユーザのことをいう。なお、ホストとゲストとは、互いの携帯端末の表示部１４に表示された内容が視認できる範囲内にいるものとする。
【００４７】
結合情報は、例えば、図３に示すように、２０４８ビットのホストの公開鍵と、１６ビットのホストの乱数と、２０４８ビットのゲストの公開鍵と、１６ビットのゲストの乱数とからなる。
【００４８】
記号生成部１３は、このような結合情報から得られた１６０ビット（一方向性関数としてＳＨＡ－１を用いた場合）のハッシュ値を１０ビット毎に分割し、１０ビットで表現される１０２４通りの数値に対応する１６個の文字列を表示部１４に表示させるようになっている。ここで、各数値にそれぞれ対応する文字列は、各携帯端末にフラッシュメモリ４等に予め共通に格納されている。
【００４９】
表示部１４は、図４に示すように、記号生成部１３によって生成された１６個の文字列を表示するようになっている。ここで、相互の携帯端末の表示部１４に表示された１６個の文字列が同一である場合には、通信部１１によって相互に交換された公開鍵は、正当なものであり、同一でない場合には、通信部１１によって相互に交換された公開鍵の少なくとも一方は、正当なものではないことが分かる。
【００５０】
したがって、相互の携帯端末のユーザは、相互の携帯端末の表示部１４に表示された１６個の文字列が同一であることを視認した場合には、入力装置５を介して、相手の公開鍵が認証された旨を入力（例えば、ＯＫボタンをクリック）し、１６個の文字列が同一でないことを視認した場合には、入力装置５を介して、相手の公開鍵が認証されなかった旨を入力（例えば、ＮＧボタンをクリック）する。このように、入力装置５は、本発明に係る認証情報受付部を構成する。
【００５１】
相手の公開鍵が認証された旨が入力装置５に入力された場合には、鍵管理部１０は、相手の公開鍵を認証された公開鍵としてフラッシュメモリ４等に格納し、相手の公開鍵が認証されなかった旨が入力装置５に入力された場合には、鍵管理部１０は、相手の公開鍵を廃棄するようになっている。
【００５２】
相手の公開鍵が認証された旨が入力装置５に入力され、この公開鍵をフラッシュメモリ４等に保存した後には、鍵管理部１０は、この公開鍵で暗号化した共通鍵を生成し、通信

部１１は、この暗号化された共通鍵を相手の携帯端末に送信し、以後、その共通鍵を用いて暗号化通信を行うようにしてもよい。

【００５３】

以上のように構成された携帯端末の公開鍵相互認証動作を図５を用いて説明する。

【００５４】

まず、ホストの携帯端末（図５左側、以下「ホスト端末」という。）において、入力装置５を介して公開鍵相互認証が要求されると、ホスト端末の通信部１１によってゲストの携帯端末（図５右側、以下「ゲスト端末」という。）に公開鍵相互認証が要求される（ステップＳ１）。

【００５５】

次に、ホスト端末において、一時共有情報生成部１２によって乱数が発生される（ステップＳ２）。一方、公開鍵相互認証が要求されたゲスト端末においても、一時共有情報生成部１２によって、乱数が発生される（ステップＳ３）。

【００５６】

ゲストの公開鍵と、一時共有情報生成部１２によって発生された乱数とは、ゲスト端末の通信部１１によってホスト端末に送信される（ステップＳ４）。一方、ホストの公開鍵と、ホスト端末の一時共有情報生成部１２によって発生された乱数とは、ホスト端末の通信部１１によってゲスト端末に送信される（ステップＳ５）。

【００５７】

ここで、ホスト端末において、ホストの公開鍵、ホストの乱数、ゲストの公開鍵およびゲストの乱数からなる結合情報のハッシュ値が記号生成部１３によって算出され（ステップＳ６）、算出されたハッシュ値から１６個の文字列が生成され（ステップＳ７）、生成された文字列が表示部１４に表示される（ステップＳ８）。

【００５８】

ゲスト端末においても同様に、ホストの公開鍵、ホストの乱数、ゲストの公開鍵およびゲストの乱数からなる結合情報のハッシュ値が記号生成部１３によって算出され（ステップＳ９）、算出されたハッシュ値から１６個の文字列が生成され（ステップＳ１０）、生成された文字列が表示部１４に表示される（ステップＳ１１）。

【００５９】

この状態で、ホストとゲストとは、双方の端末の表示部１４に表示された文字列が同一であるか否かを視認することにより、相手の公開鍵を相互に認証する。

【００６０】

ホスト端末において、相手の公開鍵が認証された旨が入力装置５に入力された場合には（ステップＳ１２：ＯＫ）、ゲストの公開鍵が認証された公開鍵として鍵管理部１０によってフラッシュメモリ４等に登録され（ステップＳ１３）、相手の公開鍵が認証されなかった旨が入力装置５に入力された場合には（ステップＳ１２：ＮＧ）、ゲストの公開鍵が鍵管理部１０によって廃棄される（ステップＳ１４）。

【００６１】

ゲスト端末においても同様に、相手の公開鍵が認証された旨が入力装置５に入力された場合には（ステップＳ１５：ＯＫ）、ホストの公開鍵が認証された公開鍵として鍵管理部１０によってフラッシュメモリ４等に登録され（ステップＳ１６）、相手の公開鍵が認証されなかった旨が入力装置５に入力された場合には（ステップＳ１５：ＮＧ）、ホストの公開鍵が鍵管理部１０によって廃棄される（ステップＳ１７）。

【００６２】

このように、本実施の形態としての携帯端末は、公開鍵相互認証時にホスト端末とゲスト端末とが乱数を発生し、発生した乱数を含む結合情報のハッシュ値から文字列を生成する。

【００６３】

このため、悪意のあるユーザが、公開鍵相互認証時の通信を傍受していたとしても、ホスト端末とゲスト端末との各表示部１４に同一の文字列を表示させる偽の公開鍵を事前に

用意しておき、公開鍵を改ざんすることは、不可能である。

【００６４】

以上に説明したように、本発明の第１の実施の形態としての携帯端末は、表示部１４に表示された情報が自己と相手とで同一のものであるか否かを視認させることで、自己の公開鍵と相手の公開鍵とを相互に認証させるため、認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる。

【００６５】

なお、本実施の形態において、結合情報は、ホストの公開鍵、ホストの乱数、ゲストの公開鍵およびゲストの乱数からなるものとして説明したが、図６（ａ）に示すように、ホストの公開鍵、ホストの乱数およびゲストの公開鍵からなるものでもよい。

【００６６】

この場合には、図５に示した公開鍵相互認証動作は、ステップＳ３が省かれ、ステップＳ４において、ゲストの公開鍵が、ゲスト端末の通信部１１によってホスト端末に送信されるように変更される。

【００６７】

また、結合情報は、図６（ｂ）に示すように、ホストの公開鍵、ゲストの公開鍵およびゲストの乱数からなるものでもよい。この場合には、図５に示した公開鍵相互認証動作は、ステップＳ２が省かれ、ステップＳ５において、ホストの公開鍵が、ホスト端末の通信部１１によってゲスト端末に送信されるように変更される。

【００６８】

また、本実施の形態において、記号生成部１３は、結合情報から得られたハッシュ値を分割し、分割した各数値に対応する文字列を表示部１４に表示させる例について説明したが、本発明においては、ハッシュ値の一部の数値（例えば、上位１６ビット）に対応する文字列（例えば、１６進表示の４桁の数値を表す文字列）を表示部１４に表示させるようにしてもよい。

【００６９】

（第２の実施の形態）

本発明の第２の実施の形態としての携帯端末においては、一時共有情報生成部１２が、入力装置５によって入力されたパスワードを一時的な共有情報とする。すなわち、入力装置５は、本発明に係る入力部を構成する。ここで、パスワードは、ホストとゲストとの間で公開鍵相互認証を行う直前に相互に取り決められることが好ましい。

【００７０】

また、本実施の形態において、記号生成部１３は、ホストの公開鍵と、ゲストの公開鍵と、パスワードとを結合した結合情報に対して、ＳＨＡ－１等の一方向性関数を用いてハッシュ値を算出するようになっている。

【００７１】

結合情報は、例えば、図７に示すように、２０４８ビットのホストの公開鍵と、２０４８ビットのゲストの公開鍵と、３２ビットのパスワードとからなる。記号生成部１３は、このような結合情報から得られた１６０ビット（一方向性関数としてＳＨＡ－１を用いた場合）のハッシュ値を１０ビット毎に分割し、１０ビットで表現される１０２４通りの数値に対応する１６個の文字列を表示部１４に表示させるようになっている。

【００７２】

以上のように構成された携帯端末の公開鍵相互認証動作を図８を用いて説明する。

【００７３】

まず、ホスト端末において、入力装置５を介して公開鍵相互認証が要求されると、ホスト端末の通信部１１によってゲスト端末に公開鍵相互認証が要求される（ステップＳ２１）。

【００７４】

次に、ホスト端末において、入力装置５を介してパスワードが入力されるのを待つ（ス

テップＳ２２）。一方、公開鍵相互認証が要求されたゲスト端末においても、入力装置５を介してパスワードが入力されるのを待つ（ステップＳ２３）。

【００７５】

ゲスト端末の入力装置５にパスワードが入力されると、ゲストの公開鍵が、ゲスト端末の通信部１１によってホスト端末に送信される（ステップＳ２４）。一方、ホスト端末の入力装置５にパスワードが入力されると、ホストの公開鍵が、ホスト端末の通信部１１によってゲスト端末に送信される（ステップＳ２５）。

【００７６】

ここで、ホスト端末において、ホストの公開鍵、ゲストの公開鍵およびパスワードからなる結合情報のハッシュ値が記号生成部１３によって算出され（ステップＳ２６）、算出されたハッシュ値から１６個の文字列が生成され（ステップＳ２７）、生成された文字列が表示部１４に表示される（ステップＳ２８）。

【００７７】

ゲスト端末においても同様に、ホストの公開鍵、ゲストの公開鍵およびパスワードからなる結合情報のハッシュ値が記号生成部１３によって算出され（ステップＳ２９）、算出されたハッシュ値から１６個の文字列が生成され（ステップＳ３０）、生成された文字列が表示部１４に表示される（ステップＳ３１）。

【００７８】

この状態で、ホストとゲストとは、双方の端末の表示部１４に表示された文字列が同一であるか否かを視認することにより、相手の公開鍵を相互に認証する。

【００７９】

ホスト端末において、相手の公開鍵が認証された旨が入力装置５に入力された場合には（ステップＳ３２：ＯＫ）、ゲストの公開鍵が認証された公開鍵として鍵管理部１０によってフラッシュメモリ４等に登録され（ステップＳ３３）、相手の公開鍵が認証されなかった旨が入力装置５に入力された場合には（ステップＳ３２：ＮＧ）、ゲストの公開鍵が鍵管理部１０によって廃棄される（ステップＳ３４）。

【００８０】

ゲスト端末においても同様に、相手の公開鍵が認証された旨が入力装置５に入力された場合には（ステップＳ３５：ＯＫ）、ホストの公開鍵が認証された公開鍵として鍵管理部１０によってフラッシュメモリ４等に登録され（ステップＳ３６）、相手の公開鍵が認証されなかった旨が入力装置５に入力された場合には（ステップＳ３５：ＮＧ）、ホストの公開鍵が鍵管理部１０によって廃棄される（ステップＳ３７）。

【００８１】

このように、本実施の形態としての携帯端末は、公開鍵相互認証前（好ましくは公開鍵相互認証直前）にホストとゲストとの間で取り決められたパスワードを含む結合情報のハッシュ値から文字列を生成する。

【００８２】

このため、悪意のあるユーザが、公開鍵相互認証時の通信を傍受していたとしても、ホスト端末とゲスト端末との各表示部１４に同一の文字列を表示させる偽の公開鍵を事前に用意しておき、公開鍵を改ざんすることは、不可能である。

【００８３】

以上に説明したように、本発明の第２の実施の形態としての携帯端末は、本発明の第１の実施の形態と同様に、表示部１４に表示された情報が自己と相手とで同一のものであるか否かを視認させることで、自己の公開鍵と相手の公開鍵とを相互に認証させるため、認証局が存在しない通信環境において、公開鍵を相互に認証させるためにユーザにかける負担を従来のものより軽減することができる。

【００８４】

なお、本実施の形態において、記号生成部１３は、結合情報から得られたハッシュ値を分割し、分割した各数値に対応する文字列を表示部１４に表示させる例について説明したが、本発明においては、ハッシュ値の一部の数値（例えば、上位１６ビット）に対応する

文字列（例えば、１６進表示の４桁の数値を表す文字列）を表示部１４に表示させるようにしてもよい。

【図面の簡単な説明】

【００８５】

【図１】本発明の実施の形態としての携帯端末のハードウェア構成図である。

【図２】本発明の実施の形態としての携帯端末の公開鍵認証にかかる機能ブロック図である。

【図３】本発明の第１の実施の形態としての携帯端末によって生成される結合情報を説明するための概念図である。

【図４】本発明の第１の実施の形態としての携帯端末を構成する表示部の表示例を示すイメージである。

【図５】本発明の第１の実施の形態としての携帯端末の公開鍵相互認証動作を示すシーケンス図である。

【図６】本発明の第１の実施の形態としての携帯端末によって生成される他の結合情報を説明するための概念図である。

【図７】本発明の第２の実施の形態としての携帯端末によって生成される結合情報を説明するための概念図である。

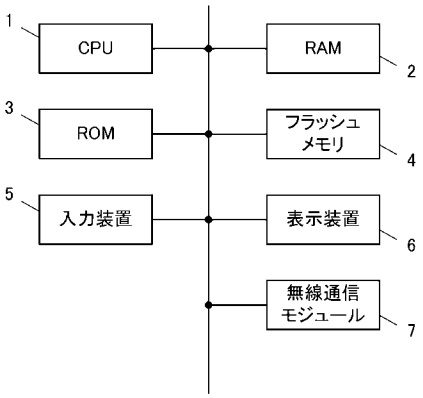
【図８】本発明の第２の実施の形態としての携帯端末の公開鍵相互認証動作を示すシーケンス図である。

【符号の説明】

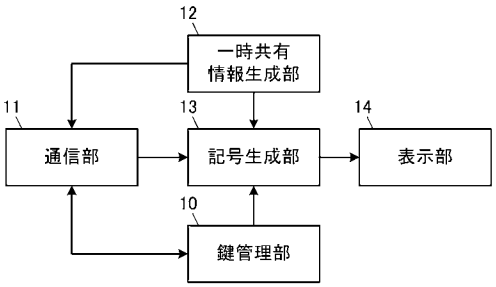
【００８６】

１　ＣＰＵ
２　ＲＡＭ
３　ＲＯＭ
４　フラッシュメモリ
５　入力装置
６　表示装置
７　無線通信モジュール
１０　鍵管理部
１１　通信部
１２　一時共有情報生成部
１３　記号生成部
１４　表示部

【図１】



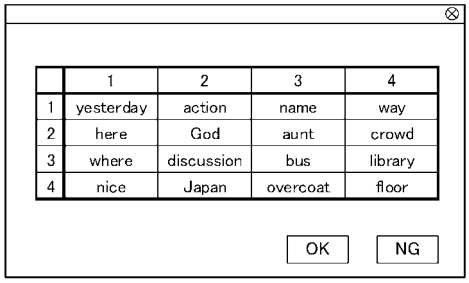
【図２】



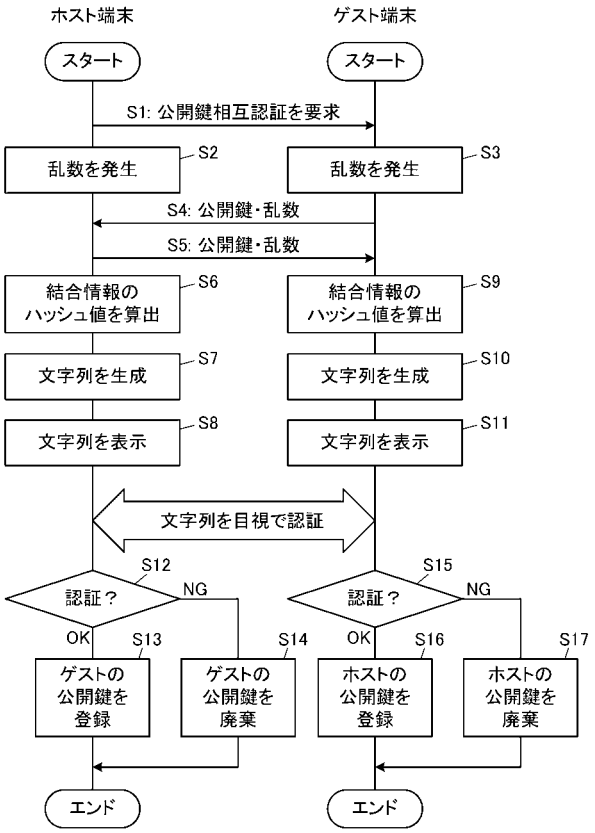
【図３】

ホストの公開鍵	ホストの乱数	ゲストの公開鍵	ゲストの乱数
2048ビット	16ビット	2048ビット	16ビット

【図４】



【図５】



【図６】

ホストの公開鍵	ホストの乱数	ゲストの公開鍵
2048ビット	16ビット	2048ビット

(a)

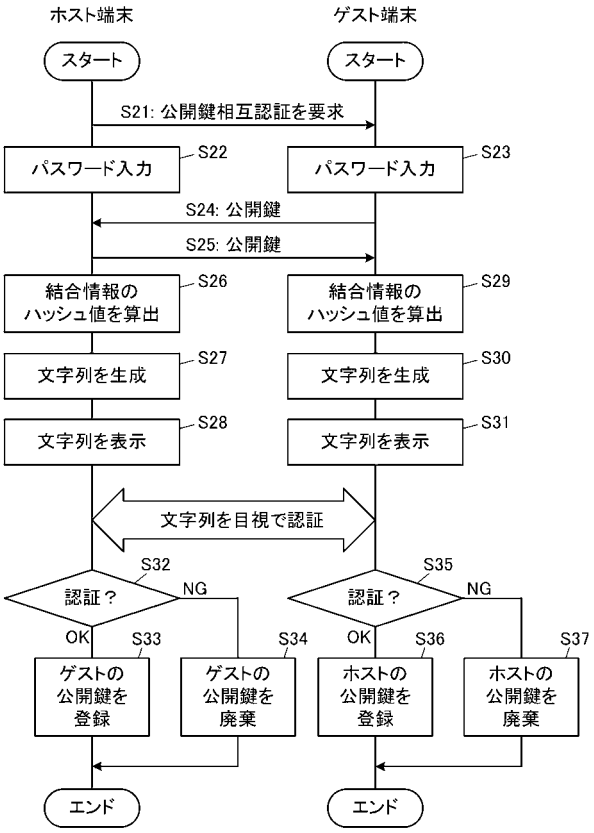
ホストの公開鍵	ゲストの公開鍵	ゲストの乱数
2048ビット	2048ビット	16ビット

(b)

【図７】

ホストの公開鍵	ゲストの公開鍵	パスワード
2048ビット	2048ビット	32ビット

【図８】


ホスト端末
ゲスト端末
スタート
スタート
S21: 公開鍵相互認証を要求
パスワード入力
S22
パスワード入力
S23
S24: 公開鍵
S25: 公開鍵
結合情報の
ハッシュ値を算出
S26
結合情報の
ハッシュ値を算出
S29
文字列を生成
S27
文字列を生成
S30
文字列を表示
S28
文字列を表示
S31
文字列を目視で認証
認証？
S32
NG
認証？
S35
NG
OK
S33
ゲストの
公開鍵を
登録
S34
ゲストの
公開鍵を
廃棄
OK
S36
ホストの
公開鍵を
登録
S37
ホストの
公開鍵を
廃棄
エンド
エンド

フロントページの続き

(72)発明者　野田　厚志
福岡県福岡市西区元岡７４４番地　国立大学法人九州大学内
(72)発明者　阿瀬川　稔
福岡県福岡市西区元岡７４４番地　国立大学法人九州大学内
(72)発明者　北須賀　輝明
熊本県熊本市黒髪ニ丁目３９番１号　国立大学法人熊本大学内

Ｆターム(参考) 5J104 AA07　AA16　EA03　EA05　EA16　KA01　KA06　KA08　KA21　NA05
NA10　NA12　NA38　PA07