(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7152466号
(P7152466)

(45)発行日　令和4年10月12日(2022.10.12)

(24)登録日　令和4年10月3日(2022.10.3)

(51)国際特許分類			FI		
Ｅ０５Ｂ	*49/00*	*(2006.01)*	Ｅ０５Ｂ	49/00	Ｊ
Ｈ０４Ｌ	*9/32*	*(2006.01)*	Ｈ０４Ｌ	9/32	２００Ａ
Ｈ０４Ｌ	*9/08*	*(2006.01)*	Ｈ０４Ｌ	9/08	Ｃ
Ｇ０６Ｆ	*21/44*	*(2013.01)*	Ｇ０６Ｆ	21/44	
Ｈ０４Ｗ	*12/06*	*(2021.01)*	Ｈ０４Ｗ	12/06	

請求項の数　14　（全29頁）

(21)出願番号　特願2020-502749(P2020-502749)
(86)(22)出願日　平成30年3月22日(2018.3.22)
(65)公表番号　特表2020-519208(P2020-519208A)
(43)公表日　令和2年6月25日(2020.6.25)
(86)国際出願番号　PCT/CN2018/079999
(87)国際公開番号　WO2018/177188
(87)国際公開日　平成30年10月4日(2018.10.4)
審査請求日　令和3年3月19日(2021.3.19)
(31)優先権主張番号　201710198457.1
(32)優先日　平成29年3月29日(2017.3.29)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　519352986
云丁网▲絡▼技▲術▼（北京）有限公司
中華人民共和国１００００９４北京市海淀区北清路８１号二区１号楼１１▲層▼１１０１室
Ｒｏｏｍ １１０１，１１ｔｈ Ｆｌｏｏｒｓ，Ｂｕｉｌｄｉｎｇ １，Ａｒｅａ ２，Ｎｏ．８１ Ｂｅｉｑｉｎｇ Ｒｏａｄ，Ｈａｉｄｉａｎ Ｄｉｓｔｒｉｃｔ，Ｂｅｉｊｉｎｇ，１００００９４，ＣＨＩＮＡ
(74)代理人　100108453
弁理士　村山 靖彦
(74)代理人　100110364
弁理士　実広 信哉

最終頁に続く

(54)【発明の名称】　セキュア通信方法及びそれに基づくスマートロックシステム

(57)【特許請求の範囲】

【請求項１】

第１のデバイスと第２のデバイスを備えるシステムであって、前記第１のデバイスは、

送信すべきデータを生成し、

前記送信すべきデータを暗号化することで暗号化データを決定し、

前記暗号化データに一意識別子を割り当て、

前記一意識別子付き暗号化データを前記第２のデバイスに送信するように構成され、前記第２のデバイスは前記第１のデバイスの対になっているデバイスであり、

前記送信すべきデータを暗号化することは、

前記第１のデバイスに記憶された第１の暗号化キーに基づいて暗号化アルゴリズムを用いて前記送信すべきデータを暗号化することで初期暗号化データを決定することであって、前記第１の暗号化キーは、前記第１のデバイスと前記第２のデバイスによる許可により起動される短距離無線通信チャネルを介して取得された、前記決定することと、

前記初期暗号化データに対して予め設定されたキー値を設定することと、

前記予め設定されたキー値で設定された前記初期暗号化データに検証署名を付加することで、前記暗号化データを決定することと、を含み、

前記第１のデバイスと前記第２のデバイスの１つはスマートドアロックであり、前記第１のデバイスと前記第２のデバイスの他の１つはモバイルデバイスであり、

前記第２のデバイスは、

前記一意識別子付き暗号化データに対して本人認証を行うことで、前記暗号化データが前

記対になっているデバイスから送信されたと判定するように構成され、
前記本人認証を行うことは、
前記一意識別子付き暗号化データから前記一意識別子を抽出することと、
前記一意識別子に対応する暗号化キーを決定することと、
前記暗号化キーが前記第２のデバイスに記憶された第２の暗号化キーと同じであるか又は対応するか否かを判定することと、
前記暗号化キーが前記第２の暗号化キーと同じであるか又は対応すると判定したことに応答して、前記暗号化データが前記対になっているデバイスから送信されたと判定することと、を含む、システム。
【請求項２】
前記第２のデバイスは、
前記暗号化データを復号することで、復号データを生成するようにさらに構成され、
前記暗号化データを復号することは、
前記暗号化データの検証署名が一致であることを検証することと、
前記予め設定されたキー値が正当であることを検証することと、
前記第２の暗号化キーを用いて前記初期暗号化データを復号することであって、前記第２の暗号化キーは、前記短距離無線通信チャネルを介して取得された、前記復号することと、を含む、請求項１に記載のシステム。
【請求項３】
前記暗号化アルゴリズムは対称暗号化アルゴリズムであり、
前記第２の暗号化キーは前記第１の暗号化キーと同じであり、
前記検証署名はハッシュ値を含む、請求項２に記載のシステム。
【請求項４】
前記送信すべきデータは、ビデオデータ、音声データ、操作命令、スマートドアロックパスワード、Ｂｌｕｅｔｏｏｔｈキー、開錠記録、履歴記録、ドアのセンサの状態、又は住宅にいる人の存在のうちの少なくとも１つを含む、請求項１から３のいずれか一項に記載のシステム。
【請求項５】
前記一意識別子付き暗号化データを第２のデバイスに送信するために、前記第１のデバイスは、前記短距離無線通信チャネル又はサーバを介して前記一意識別子付き暗号化データを前記第１のデバイスから前記第２のデバイスに送信するように構成された、請求項１から４のいずれか一項に記載のシステム。
【請求項６】
前記第１の暗号化キー及び前記第２の暗号化キーは、前記第１のデバイスと前記第２のデバイスによって初期暗号化キーを認証することで決定され、
前記初期暗号化キーは、前記第１のデバイス又は前記第２のデバイスによって自動的に生成されるか、又は手動で入力され、
前記初期暗号化キーは、前記短距離無線通信チャネルを介して前記第１のデバイスと前記第２のデバイスの間で送信される、請求項２から５のいずれか一項に記載のシステム。
【請求項７】
前記予め設定されたキー値は、タイムスタンプ、カウンタ値又はランダムコードのうちの少なくとも１つである、請求項１から６のいずれか一項に記載のシステム。
【請求項８】
方法であって、
第１のデバイスによって、送信すべきデータを生成することと、
前記第１のデバイスによって、前記送信すべきデータを暗号化することで暗号化データを決定することと、
前記第１のデバイスによって、前記暗号化データに一意識別子を割り当てることと、
前記第１のデバイスによって、前記一意識別子付き暗号化データを第２のデバイスに送信することと、を含み、前記第２のデバイスは前記第１のデバイスの対になっているデバ

イスであり、
前記送信すべきデータを暗号化することは、
前記第１のデバイスに記憶された第１の暗号化キーに基づいて暗号化アルゴリズムを用いて前記送信すべきデータを暗号化することで初期暗号化データを決定することであって、前記第１の暗号化キーは、前記第１のデバイスと前記第２のデバイスによる許可により起動される短距離無線通信チャネルを介して取得された、前記決定することと、
前記初期暗号化データに対して予め設定されたキー値を設定することと、
前記予め設定されたキー値で設定された前記初期暗号化データに検証署名を付加することで、前記暗号化データを決定することと、を含み、
前記第１のデバイスと前記第２のデバイスの１つはスマートドアロックであり、前記第１のデバイスと前記第２のデバイスの他の１つはモバイルデバイスであり、
前記方法は、前記第２のデバイスによって、
前記一意識別子付き暗号化データに対して本人認証を行うことで、前記暗号化データが前記対になっているデバイスから送信されたと判定すること、をさらに含み、
前記本人認証を行うことは、
前記一意識別子付き暗号化データから前記一意識別子を抽出することと、
前記一意識別子に対応する暗号化キーを決定することと、
前記暗号化キーが前記第２のデバイスに記憶された第２の暗号化キーと同じであるか又は対応するか否かを判定することと、
前記暗号化キーが前記第２の暗号化キーと同じであるか又は対応すると判定したことに応答して、前記暗号化データが前記対になっているデバイスから送信されたと判定することと、を含む、方法。
【請求項９】
前記暗号化データを復号することで、復号データを生成することと、をさらに含み、
前記暗号化データを復号することは、
前記暗号化データの検証署名が一致であることを検証することと、
前記予め設定されたキー値が正当であることを検証することと、
前記第２の暗号化キーを用いて前記初期暗号化データを復号することであって、前記第２の暗号化キーは、前記短距離無線通信チャネルを介して取得された、前記復号することと、を含む、請求項８に記載の方法。
【請求項１０】
前記暗号化アルゴリズムは対称暗号化アルゴリズムであり、
前記第２の暗号化キーは前記第１の暗号化キーと同じであり、
前記検証署名はハッシュ値を含む、請求項９に記載の方法。
【請求項１１】
前記送信すべきデータは、ビデオデータ、音声データ、操作命令、スマートドアロックパスワード、Ｂｌｕｅｔｏｏｔｈキー、開錠記録、履歴記録、ドアのセンサの状態、又は住宅にいる人の存在のうちの少なくとも１つを含む、請求項８から１０のいずれか一項に記載の方法。
【請求項１２】
前記第１のデバイスによって、前記一意識別子付き暗号化データを第２のデバイスに送信することは、
前記第１のデバイスによって、前記短距離無線通信チャネル又はサーバを介して前記一意識別子付き暗号化データを前記第１のデバイスから前記第２のデバイスに送信することを含む、請求項８から１１のいずれか一項に記載の方法。
【請求項１３】
前記第１のデバイス又は前記第２のデバイスによって、初期暗号化キーを生成することと、
前記第１のデバイス及び前記第２のデバイスによって、前記短距離無線通信チャネルを介して前記第１のデバイスと前記第２のデバイスの間で前記初期暗号化キーに基づいてキ

ー交換プロセスを行うことと、
前記第１のデバイスによって、前記初期暗号化キーを認証することで前記第１の暗号化キーを決定することと、
前記第２のデバイスによって、前記初期暗号化キーを認証することで前記第２の暗号化キーを決定することと、をさらに含む、請求項９から１２のいずれか一項に記載の方法。
【請求項１４】
実行可能命令を含む非一時的コンピュータ可読媒体であって、第１のデバイスの少なくとも１つのプロセッサによって実行されるとき、前記実行可能命令は、前記少なくとも１つのプロセッサに、
送信すべきデータを生成することと、
前記送信すべきデータを暗号化することで暗号化データを決定することと、
前記暗号化データに一意識別子を割り当てることと、
前記一意識別子付き暗号化データを第２のデバイスに送信することと、を含む方法を実行させ、前記第２のデバイスは前記第１のデバイスの対になっているデバイスであり、
前記送信すべきデータを暗号化することは、
前記第１のデバイスに記憶された第１の暗号化キーに基づいて暗号化アルゴリズムを用いて前記送信すべきデータを暗号化することで初期暗号化データを決定することであって、前記第１の暗号化キーは、前記第１のデバイスと前記第２のデバイスによる許可により起動される短距離無線通信チャネルを介して取得された、前記決定することと、
前記初期暗号化データに対して予め設定されたキー値を設定することと、
前記予め設定されたキー値で設定された前記初期暗号化データに検証署名を付加することで、前記暗号化データを決定することと、を含み、
前記第１のデバイスと前記第２のデバイスの１つはスマートドアロックであり、前記第１のデバイスと前記第２のデバイスの他の１つはモバイルデバイスであり、
前記方法は、前記第２のデバイスによって、
前記一意識別子付き暗号化データに対して本人認証を行うことで、前記暗号化データが前記対になっているデバイスから送信されたと判定すること、をさらに含み、
前記本人認証を行うことは、
前記一意識別子付き暗号化データから前記一意識別子を抽出することと、
前記一意識別子に対応する暗号化キーを決定することと、
前記暗号化キーが前記第２のデバイスに記憶された第２の暗号化キーと同じであるか又は対応するか否かを判定することと、
前記暗号化キーが前記第２の暗号化キーと同じであるか又は対応すると判定したことに応答して、前記暗号化データが前記対になっているデバイスから送信されたと判定することと、を含む、非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
＜関連出願の相互参照＞
本出願は、アメリカ合衆国を指定国として２０１８年３月２２日に出願された国際特許出願第ＰＣＴ／ＣＮ２０１８／０７９９９９号の継続出願であり、２０１７年３月２９日に出願された中国特許出願第２０１７１０１９８４５７．１号の優先権を主張し、その全体は参照により本明細書に援用される。
【０００２】
本開示は、概して、スマートホーム及び安全監視の分野におけるセキュア通信技術に関する。
【背景技術】
【０００３】
市場で現在利用可能なスマートドアロックは、通信機能を備えている。スマートドアロックの情報は、サーバに送信され、次に、ユーザによって使用されるアプリケーション（

アプリ）などに転送され得る。ユーザは、サーバを介して、遠隔的にパスワードを発行したり、許可を与えたりすることもできる。スマートドアロックが多く取り付けられるほど、遠隔通信の安全性が重要になっている。通信のセンターとして、サーバは攻撃される危険性が高く、パスワードの漏洩やドアが適切な許可なしで開かれることなどの重大な事故になるおそれがある。

【０００４】

これらの問題に対処するために、以下のような既存の解決策がある。

【０００５】

（１）遠隔開錠機能を禁止する。しかし、ほとんどのスマートドアロックは、パスワード、Ｂｌｕｅｔｏｏｔｈ（登録商標、以下同じ）キーなどを遠隔的に発行することができる。サーバが攻撃された場合、攻撃されたサーバによりスマートロックにパスワードやＢｌｕｅｔｏｏｔｈキーを発行させることで、開錠許可を取得し、次にローカルに開錠操作を行うことができる。

【０００６】

（２）ドアロックとサーバとの間で暗号化通信を用いて、ユーザアプリとサーバとの間の通信にもＨＴＴＰＳなどの暗号化技術を用いる。この方法は、通信ネットワークにおけるデータ送信中のデータ取り込みを防ぐことができるが、パスワード及びＢｌｕｅｔｏｏｔｈキーなどのキー情報がサーバに記憶されているので、攻撃者はサーバからパスワード及びＢｌｕｅｔｏｏｔｈキーを取得することができる。同時に、本人認証、アンチリプレイ、改ざん防止の機能がなければ、サーバが攻撃された場合にドアロックやモバイル端末にどのように関連するコマンドを発行するかという問題は解決されない。

【０００７】

（３）サーバとモバイル端末又はドアロックとの間の通信に、アンチリプレイ機能及び改ざん防止機能を採用する。しかし、サーバが侵害されたので、サーバとモバイル端末又はドアロックとの間の正常な通信をシミュレートすることが可能で、サーバ側での本人認証を遮断することはできない。

【０００８】

現在、市場では、サーバやスタッフメンバーがサーバからユーザの送信情報を取得することを防止したり、サーバのセキュリティが破壊されたりしても、ドアロックとモバイル端末との間の通信における本人認証、アンチリプレイ、改ざん防止の機能を維持できるセキュア通信技術が得られない。

【発明の概要】

【課題を解決するための手段】

【０００９】

本開示は、上述の欠点を克服するスマートドアロックシステムに適用可能なセキュア通信方法を提供する。その技術的解決策は以下の通りである。

【００１０】

本開示の第１の態様によれば、スマートドアロックとモバイル端末とを含むことができるスマートドアロックシステムに適用可能なセキュア通信方法を提供し、該方法は、

前記スマートドアロック又は前記モバイル端末である送信端末によって、操作命令又は予め設定されたルールに従って、送信すべきデータを生成し、前記スマートドアロックと前記モバイル端末による許可により起動される短距離無線通信チャネル又は近距離無線通信（ＮＦＣ）チャネルである予め設定されたセキュア通信チャネルを介してスマートドアロックとモバイル端末との間のキー交換プロセスによって取得された暗号化キーに基づいて予め設定された暗号化アルゴリズムを用いて送信すべきデータを暗号化することで、暗号化データを決定することと、

送信端末によって暗号化データに一意識別子を割り当てることと、

送信端末によって一意識別子付き暗号化データを受信端末に送信することで、受信端末によって一意識別子付き暗号化データに対して本人認証を行い、本人認証の結果に応じて暗号化キーを用いて暗号化データを復号することと、を含む。

【００１１】
送信端末はスマートドアロックを含み、受信端末はモバイル端末を含み、あるいは、送信端末はモバイル端末を含み、受信端末はスマートドアロックを含むことができる。
【００１２】
いくつかの実施形態では、送信端末によって一意識別子付き暗号化データを受信端末に送信することは、
送信端末によって、一意識別子付き暗号化データを、短距離無線通信チャネル又はＮＦＣチャネルを含む予め設定されたセキュア通信チャネル又はクラウドサーバを介して、受信端末に送信することを含む。
【００１３】
いくつかの実施形態では、暗号化キーは、スマートドアロックとモバイル端末によって初期暗号化キーを認証することで決定することができ、初期暗号化キーは、スマートドアロック又はモバイル端末がユーザーの許可命令に応答して生成することができ、初期暗号化キーは、スマートドアロック又はモバイル端末によって自動的に生成されるか、又は手動で入力されるキーであり、予め設定されたセキュア通信チャネルを介してスマートドアロックとモバイル端末との間で送信されることができる。
【００１４】
いくつかの実施形態では、暗号化キーは、第１の暗号化キーを含み、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化することで暗号化データを決定することは、
対称暗号化アルゴリズムを用いて第１の暗号化キーに基づいて送信すべきデータを暗号化することで初期暗号化データを決定することと、
初期暗号化データに対して、タイムスタンプ、カウンタ値又はランダムコードのうちの少なくとも１つである予め設定されたキー値を設定することと、
予め設定されたキー値で設定された初期暗号化データに検証署名を付加することで、暗号化データを決定することと、を含む。
【００１５】
いくつかの実施形態では、送信端末と受信端末に記憶された暗号化キーは、それぞれ公開キーと秘密キーを含み、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化することで暗号化データを決定することは、
送信端末によって、非対照暗号化アルゴリズムを用いて送信端末に記憶された公開キーに基づいて送信すべきデータを暗号化することで初期暗号化データを決定することと、
初期暗号化データに対して、タイムスタンプ、カウンタ値又はランダムコードのうちの少なくとも１つである予め設定されたキー値を設定することと、
送信端末に記憶された秘密キーを検証署名として、予め設定されたキー値で設定された初期暗号化データに付加することで、暗号化データを決定すること、とを含む。
【００１６】
いくつかの実施形態では、該方法はさらに、
モバイル端末のバックアップデバイスであるバックアップモバイル端末によって、ユーザの本人性を検証するための情報を含むアカウントログイン検証情報を取得することと、
アカウントログイン検証情報が検証された場合、バックアップモバイル端末によって、ユーザによる削除操作の許可に応答して、スマートドアロックに第１の削除命令を送信して、ローカルに記憶された暗号化キー情報を削除するようスマートドアロックに命令し、及び／又は、バックアップモバイル端末によって、ユーザによる削除操作の遠隔許可に応答して、クラウドサーバに第２の削除命令を送信して、モバイル端末に記憶された暗号化キー情報を削除するようクラウドサーバに命令することと、を含む。
【００１７】
本開示の第２の態様によれば、セキュア通信のための方法を提供する。該方法は、スマートドアロックとモバイル端末とを含むスマートドアロックシステムに適用することができる。該方法は、

受信端末によって、送信端末が送信した一意識別子付き暗号化データを受信することと、
受信端末によって、一意識別子付き暗号化データに対して本人認証を行うことで、本人認証の結果を決定することと、
受信端末によって、本人認証の結果に応じて、キー交換プロセスにより取得された暗号化キーを用いて暗号化データを復号することで送信すべきデータを決定することと、を含み、送信端末はスマートドアロックを含み、受信端末はモバイル端末を含み、あるいは、送信端末はモバイル端末を含み、受信端末はスマートドアロックを含み、一意識別子付き暗号化データは、送信端末によって、操作命令又は予め設定されたルールに従って、送信すべきデータを決定し、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化することで暗号化データを決定し、暗号化データに一意識別子を割り当てることによって、決定され、暗号化キーは、予め設定されたセキュア通信チャネルを介してスマートドアロックとモバイル端末との間のキー交換プロセスによって取得され、予め設定されたセキュア通信チャネルは、スマートドアロックとモバイル端末による許可により起動される短距離無線通信チャネル又は近距離無線通信（ＮＦＣ）チャネルである。

【００１８】

いくつかの実施形態では、暗号化キーは第１の暗号化キーであり、暗号化データは、対称暗号化アルゴリズムを用いて第１の暗号化キーに基づいて送信すべきデータを暗号化することで初期暗号化データを決定し、初期暗号化データに対して、予め設定されたキー値を設定し、予め設定されたキー値で設定された初期暗号化データに検証署名を付加することによって、決定され、
受信端末によって、本人認証の結果に応じて、交換により取得された暗号化キーを用いて暗号化データを復号することで送信すべきデータを決定することは、
本人認証の結果が一致である場合、受信端末が暗号化データの署名を検証し、
署名検証の結果が一致である場合、受信端末が予め設定されたキー値が正当であるかを検証し、
予め設定されたキー値が正当であれば、受信端末が、暗号化データから初期暗号化データを取得するとともに、対称暗号化アルゴリズムの逆のアルゴリズムを用いて第１の暗号化キーに基づいて初期暗号化データを復号することで送信すべきデータを決定することを含む。

【００１９】

いくつかの実施形態では、送信端末と受信端末に記憶された暗号化キーは、それぞれ公開キーと秘密キーを含む。暗号化データは、対称暗号化アルゴリズムを用いて送信端末に記憶された公開キーに基づいて送信すべきデータを暗号化することで初期暗号化データを決定し、初期暗号化データに対して、予め設定されたキー値を設定し、送信端末に記憶された秘密キーを検証署名として、予め設定されたキー値で設定された初期暗号化データに付加することによって、決定され、
受信端末によって、本人認証の結果に応じて、キー交換プロセスにより取得された暗号化キーを用いて暗号化データを復号することで送信すべきデータを決定することは、
本人認証の結果が一致である場合、受信端末が受信端末に記憶された公開キーを用いて暗号化データの検証署名を検証し、
署名検証の結果が一致である場合、受信端末が予め設定されたキー値が正当であるかを検証し、
予め設定されたキー値が正当であれば、受信端末が、暗号化データから初期暗号化データを取得するとともに、非対称暗号化アルゴリズムを用いて第１の暗号化キーに基づいて初期暗号化データを復号することで送信すべきデータを決定することを含む。

【００２０】

いくつかの実施形態では、受信端末によって、一意識別子付き暗号化データに対して本人認証を行うことは、
受信端末によって、一意識別子付き暗号化データから一意識別子を抽出することと、

一意識別子分析により一意識別子に一致する暗号化キーを取得することと、
暗号化キーに基づいて本人認証の結果を決定することと、を含む。
【００２１】
本開示の第３の態様によれば、スマートドアロックシステムを提供する。スマートドアロックシステムは、
暗号化キーを用いて送信すべきデータを暗号化し、予め設定された暗号化アルゴリズムにより、受信した暗号化データを復号するように構成され、短距離無線通信モジュールを含むスマートドアロックと、
暗号化キーを用いて送信すべきデータを暗号化し、スマートドアロックと同様の予め設定された暗号化アルゴリズムにより、受信した暗号化データを復号するように構成され、さらに、スマートドアロックを制御するように構成され、スマートドアロックと通信するための短距離無線通信モジュールを含むモバイル端末と、を含む。
【００２２】
いくつかの実施形態では、スマートドアロックは、暗号化キーを生成し交換するために設定モードを起動するように構成された設定モード起動モジュールをさらに含む。設定モード起動モジュールは、設定ボタン、設定モードタッチキー、管理者パスワードを入力するためのタッチスクリーン又は管理者の指紋を入力するための指紋コレクターのうちの少なくとも１つを含む。
【００２３】
いくつかの実施形態では、モバイル端末によってスマートドアロックを制御することは、スマートドアロック制御アプリでスマートドアロックを制御することを含んでもよく、スマートドアロック制御アプリは、モバイル端末の設定モードを起動するように構成された設定モードを起動するための仮想ボタンを含むことができる。
【００２４】
本開示のスマートドアロックシステムに適用可能なセキュア通信方法によれば、スマートドアロックもモバイル端末もユーザの許可でセキュア通信を起動することができる。即ち、スマートドアロックと各モバイル端末のアプリは、ユーザの許可で短距離無線通信チャネル又は近距離無線通信（ＮＦＣ）チャネルを介して暗号化キーを送信して交換し、したがって、暗号化キーの安全な交換を可能にする。スマートドアロックと各モバイル端末のアプリに同様の又は対応する暗号化アルゴリズムを設定することができる。暗号化アルゴリズムを用いてローカルに暗号化及び復号プロセスを行って、エンドツーエンドの暗号化通信を達成することができる。サーバエンド又はスマートドアロック製造業者の内部職員がユーザにより送信された情報をサーバから取得することを、防止することができる。サーバが侵害された場合であっても、ドアロックとモバイル端末との間の通信における本人認証、アンチリプレイ及び改ざん防止の機能が有効に保ち、ユーザ情報を保護することができる。モバイル端末とスマートドアロックとの間で短距離無線通信又はＮＦＣチャネルを介して暗号化キーの生成及び交換をローカルに行うため、サーバは暗号化キーに関連する情報を記憶せず、サーバにより転送されるデータを復号することができず、データセキュリティが保護される。サーバが攻撃され誰かがサーバ又はサーバの通信ネットワークを介してモバイル端末又はドアロックに偽のコマンドを送信しても、本人認証の失敗のため、モバイル端末もドアロックも応答しない。誰かがサーバ又はサーバの通信ネットワークにおいてコマンドをリプレイ又は改ざんする場合、モバイル端末又はドアロックは分析して、応答しないようと決定ことができる。上記で例示した攻撃が発生した場合、モバイル端末又はドアロックは、必要に応じてサーバに又はローカルに警報を送信することができる。
【００２５】
以上の説明はただ本開示技術的解決策の概要である。例示のために、明細書において本開示の技術的特徴を提供したが、以下は、本開示の実施形態である。
【００２６】
以下の例示的な実施形態の詳細な説明を読むことにより、様々な他の優位性及び有益性

は当業者にとって明瞭になる。図面は、例示及び説明のみを目的とし、本開示の範囲を限定することを意図するものではない。また、図面のいくつかの図を通して、同様の符号は同様の構造を表す。図面において、

【図面の簡単な説明】

【００２７】

【図１】本開示のいくつかの実施形態に係る例示的なスマートドアロックシステムを示す概略構造図

【図２】本開示のいくつかの実施形態に係る例示的なスマートドアロックシステムに適用可能なセキュア通信方法を示す概略フロー図

【図３】本開示の操作Ｓ１０３の例示的な実施形態を示す概略フロー図

【図４】本開示の操作Ｓ１０７の例示的な実施形態を示す概略フロー図

【発明を実施するための形態】

【００２８】

本開示は、スマートドアロックの開錠方法を提供する。

【００２９】

当業者が本開示をより良く理解できるようにするために、以下、本開示のいくつかの実施形態における技術的解決策を、本開示の図面を参照しながら明確かつ完全に説明する。明らかに、説明した実施形態は本開示の全部の実施形態ではなく、一部のみである。本開示の実施形態に基づいて当業者によって得られる任意の他の実施形態は、本開示の範囲に属する。

【００３０】

本明細書で使用するとき、「第１」、「第２」、「第３」、「第４」など（存在する場合）の用語は、類似の物を区別するためのものであり、必ずしも特定の順序を説明するためのものではない。このように使用されたデータは、本明細書で説明された実施形態が、本明細書で図示又は説明された順番以外の順番で実施できるように適切な場合に交換され得ることがさらに理解されよう。さらに、「含む」、「有する」、及びそれらの任意の変形は、非排他的な包含をカバーしようとするものであり、例えば、一連の動作又はユニットを含むプロセス、方法、システム、製品又はデバイスは、明らかに挙げられた動作又はユニットに必ずしも限定されず、明確に挙げられていないか又はそのようなプロセス、方法、製品又はデバイスに固有の、他の動作又はユニットを含んでもよい。以下、本開示の例示的な実施形態について、図面を参照しながらさらに詳細に説明する。例示的な実施形態を本開示の図面に示しているが、本発明は、様々な形態で実施さることができ、本明細書で説明された実施形態に限定されないことが理解されよう。むしろ、これらの実施形態は、当業者に本開示がより完全に理解され、本開示の範囲が十分に開示されるように提供するものである。

【００３１】

スマートドアロックシステムの上記の説明は、例示的なものであって、本開示の範囲を限定するものではないことに留意されたい。スマートドアロックシステムの上記の説明は、例えば車両、ドア、建物、インテリジェントホーム等を含む様々な場面に適用することができる。例えば、スマートロックは、自動車ドアロック（例えば共有自動車又は私有自動車のロック）、自転車ロック（例えば共有自転車又は私有自転車のロック）、アパート／ルーム／ハウスのドアロック（例えば、共有のアパート／ルーム／ハウス又は私有アパート／ルーム／ハウスのロック）、共有又は私有のクローゼット或いはロッカーのロックなどであってもよい。本明細書で開示されるセキュア通信方法は、例示の目的のためにスマートロックである場合について説明したが、限定を意図するものではないことに留意されたい。本明細書で開示されるセキュア通信方法は、例えば、データ交換におけるアクセス認証、キー交換、デバイス間通信又はマルチデバイスからマルチデバイスへの通信などを含む様々な場面に適用することができる。該通信方法は、少なくとも２つのデバイス（第１のデバイスと第２のデバイス）の間のセキュア通信、例えばアプリケーションデバイスとモバイルデバイス（又はモバイル端末）との間、２つのモバイルデバイス（又はモバ

イル端末）の間、又は２つのアプリケーションデバイスの間のセキュア通信を容易にするために使用することができる。アプリケーションデバイスは、インテリジェントデバイス又は非インテリジェントデバイスである。アプリケーションデバイスは、ロック、ビデオドアベル、カメラ、監視装置、インテリジェントスピーカ、インテリジェント電源スイッチ、照明装置、インテリジェントゲートウェイ、環境用電気機器（例えば、エアクリーナ）、センサ、台所器具、娯楽機器、家電（例えば洗濯機）、健康監視装置（例えば血圧計）などである。第１のデバイスと第２のデバイスの１つは送信端末であり、他の１つは受信端末であることが可能である。少なくとも２つのデバイスは、マルチウェイ（例えばツーウェイ）通信に含まれることが可能である。例えば、送信端末及び受信端末の各々は、セキュア通信において、ロックを操作（例えば施錠又は開錠）するためにデータ又は情報を送受信し、許可を得て情報を交換するなどができる。送信端末又は受信端末により送受信されたデータは、アプリケーションデバイス（例えばモバイルデバイス）のパスワード、命令、データパッケージなどであることが可能である。例えば、アプリケーションデバイス（例えばモバイルデバイス）は、送信すべきデータ（例えばパスワード、ビデオデータ、音声データ、操作命令など）を生成することができ、送信すべきデータは、本開示において説明した通信方法を用いてモバイルデバイス（又はアプリケーションデバイス）に送信することができる。

【００３２】

図１を参照すると、本開示のいくつかの実施形態に係る例示的なスマートドアロックシステムを例示する概略構成図である。図１に示すように、

本開示のスマートドアロックシステムは、クラウドサーバに遠隔に接続されたスマートドアロックとモバイル端末とを含むことが可能である。

【００３３】

スマートドアロックは、予め設定された暗号化アルゴリズムを含むように構成され、予め設定された暗号化アルゴリズムは、送信すべきデータを暗号化し、受信した暗号化データを復号するように構成され、スマートドアロックは、Ｂｌｕｅｔｏｏｔｈ通信モジュール、Ｚｉｇｂｅｅ通信モジュール、又は近距離無線通信（ＮＦＣ）通信モジュールのうちの少なくとも１つを含み、

モバイル端末は、Ｂｌｕｅｔｏｏｔｈ通信モジュール、Ｚｉｇｂｅｅ通信モジュール、又は近距離無線通信（ＮＦＣ）通信モジュールのうちの少なくとも１つを含み、スマートドアロックの予め設定された暗号化アルゴリズムと同じ予め設定された暗号化アルゴリズムを含むように構成され、予め設定された暗号化アルゴリズムは、送信すべきデータを暗号化し、受信した暗号化データを復号するように構成され、

クラウドサーバは、スマートドアロックとモバイル端末との間でデータを送信するように構成される。

【００３４】

スマートドアロックシステムの上記の説明は、例示的なものであって、本開示の範囲を限定するものではないことに留意されたい。多くの代替形態、修正形態、及び変形形態は当業者にとって明らかであろう。モバイル端末は、タブレットコンピュータ、ラップトップコンピュータ、携帯電話、携帯情報端末（ＰＤＡ）、スマートウォッチ、ポイントオブセール（ＰＯＳ）デバイス、オンボードコンピュータ、車載テレビ、ウェアラブルデバイスなど、又はそれらの任意の組合せを含む。本開示において説明したクラウドサーバは、他の装置又はコンピュータプログラムに置き換えてもよい。デバイス又はコンピュータプログラムは、スマートドアロック及び／又はモバイル端末にサービスを提供することができる。デバイス又はコンピュータプログラムは、従来のサーバ、ｅｌａｓｔｉｃ ｃｏｍｐｕｔｅｒ ｓｅｒｖｉｃｅ（ＥＣＳ）、ウェブサーバ、アプリケーションサーバ、プロキシサーバ、メールサーバ、仮想サーバ、ブレードサーバ、ファイルサーバ、又はポリシーサーバなど、又はそれらの任意の組合せである。

【００３５】

いくつかの実施形態では、短距離無線通信モジュールは、Ｂｌｕｅｔｏｏｔｈ通信、Ｚ

ｉｇｂｅｅ通信モジュール、又はＮＦＣ通信モジュールのうちの少なくとも１つを含む。近距離無線通信モジュールに基づいて、予め設定された通信チャネルを確立することができる。予め設定された通信チャネルは短距離無線通信又はＮＦＣチャネルである。スマートドアロックとモバイル端末は、予め設定された通信チャネルを介してデータを送信することができ、例えば、スマートドアロック又はモバイル端末は、予め設定された通信チャネルを介して暗号化データを送信することができる。

【００３６】

いくつかの実施形態では、Ｂｌｕｅｔｏｏｔｈ通信、Ｚｉｇｂｅｅ通信モジュール、又は近距離無線通信（ＮＦＣ）通信モジュールのうちの少なくとも１つは、いくつかの他の通信モジュールで置き換えてもよい。追加として、又は代替として、スマートドアロックとモバイル端末は、短距離ワイヤレス通信モジュール、モバイルインターネット通信モジュール、従来のインターネット通信モジュール、有線シリアル通信モジュールなど、又はそれらの任意の組合せを含むことが可能である。例えば、スマートドアロック及び／又はモバイル端末は、モノのインターネットの狭帯域（ＮＢ－ＩｏＴ）通信回路、セルラーネットワーク通信回路、ＷｉＦｉ通信回路、無線周波数識別回路など、又はそれらの組合せを含むことができる。

【００３７】

本開示のいくつかの実施形態では、スマートドアロックシステムは、クラウドサーバをさらに含むことができ、モバイル端末とスマートドアロックは、クラウドサーバを介して遠隔でデータを送信することができる。

【００３８】

スマートドアロックは、暗号化キーを生成し交換するために設定モードを起動するように構成された設定モード起動モジュールをさらに含むことができる。設定モード起動モジュールは、設定ボタン、設定モードタッチキー、管理者パスワードを入力するためのタッチスクリーン又は管理者の指紋を入力するための指紋コレクターのうちの少なくとも１つと、

スマートドアロックを制御するための、モバイル端末のアプリであって、設定モードを起動するための仮想ボタンを含むように構成され、仮想ボタンが、モバイル端末の設定モードを起動するように構成されているものと、を含み、

スマートドアロックシステムは、スマートドアロックシステムに基づく以下のセキュア通信方法を実施するように構成されることが可能である。

【００３９】

いくつかの実施形態では、スマートロックは、警告モジュール、記憶モジュール、処理モジュール、ディスプレイモジュール、入力モジュールなど、又はそれらの組合せをさらに含むことができる。例えば、スマートロックは、ユーザがパスワードを入力できるようにキーパッドを含むことができる。

【００４０】

いくつかの実施形態では、モバイル端末のアプリは、スマートロックアプリであることが可能である。スマートロックアプリは、ユーザによって設定された１つ又は複数のアカウントに対応することができる。１つ又は複数のアカウントは、１つ又は複数のスマートドアロックに対応することができる。

【００４１】

スマートドアロックシステムの上記の説明は、例示的なものであって、本開示の範囲を限定するものではないことに留意されたい。多くの代替形態、修正形態、及び変形形態は当業者にとって明らかであろう。いくつかの実施形態では、クラウドサーバを省略し、データは、予め設定されたセキュア通信チャネルを介して送信してもよい。

【００４２】

図２を参照すると、本開示の例示的なスマートドアロックシステムに適用可能なセキュア通信方法を示す概略フロー図である。図２に示すように、本開示のスマートドアロックシステムに適用可能なセキュア通信方法は、

操作Ｓ１０２：スマートドアロックとモバイル端末が、予め設定されたセキュア通信チャネルを介して暗号化キーを交換することを含むことができる。予め設定されたセキュア通信チャネルは、スマートドアロックとモバイル端末の許可によって起動される通信チャネルである。セキュア通信チャネルは、短距離無線通信チャネル又はＮＦＣチャネルを含むことができる。例えば、セキュア通信チャネルは、ＷｉＦｉローカルエリアネットワーク、Ｂｌｕｅｔｏｏｔｈチャネル、Ｚｉｇｂｅｅチャネル、又はＮＦＣチャネルのうちの１つを含むことができる。

【００４３】

本開示のいくつかの実施形態では、スマートドアロックは、複数のモバイル端末に対応することができ、ユーザは、複数のモバイル端末のうちの任意の１つを用いてスマートドアロックを制御することができる。スマートドアロックが３つのモバイル端末と対になっている場合、各モバイル端末はスマートドアロックアプリをインストールされて、各アプリはアカウントに対応することができる。スマートドアロックアプリを備えるスマートドアロックとモバイル端末は、スマートドアロックとモバイル端末の許可によって起動される通信チャネルを介して通信することができる。例えば、スマートドアロックアプリを備えるスマートドアロックとモバイル端末は、許可された後に設定モードに入り、その後、独立した暗号化キーを、短距離無線通信チャネル又はＮＦＣチャネルを介して別々に交換することができる。暗号化キーは、送信すべきデータを暗号化するために用いることができる。暗号化キーは、対称キーであっても非対称キーであってもよい。モバイル端末は、スマートフォン、タブレットコンピュータ（ｉＰａｄ（登録商標））、スマートウォッチ、又はスマートドアロックアプリが予め設定されたリストバンド、小型コントローラなど、又はそれらの任意の組合せを含むが、これらに限定されない。スマートドアロックとモバイル端末は、いくつかの設定要件に従って通信モジュールを設定することができる。例えば、スマートドアロックアプリを備える携帯電話Ａは、Ｂｌｕｅｔｏｏｔｈモジュールを起動することができ、スマートドアロックは、Ｂｌｕｅｔｏｏｔｈモジュールを起動して、予め生成された暗号化キーをＢｌｕｅｔｏｏｔｈ通信により交換することができる。暗号化キーの生成はモバイル端末とスマートドアロックでローカルに行われ、暗号化キーの交換は短距離無線通信チャネル又はＮＦＣチャネルを介して行われるため、サーバが何らかの関連キーを含む場合でも、サーバは、それによって転送されたデータを理解できず、データの安全性が確保される。

【００４４】

交換された暗号化キーは、スマートドアロック及び携帯電話に暗号化キー情報として記憶することができる。暗号化キー情報は、交換された暗号化キーと、スマートドアロック又は携帯電話の一意識別子とを含むことができる。例えば、スマートドアロック（又はモバイルデバイス）は、暗号化キーを受信したモバイルデバイス（又はスマートドアドック）の、暗号化キー及び一意識別子を記憶することができる。別の例として、スマートドアロック（又はモバイルデバイス）は、暗号化キーを送信する先であったモバイルデバイス（又はスマートドアドック）の、暗号化キー及び一意識別子を記憶することができる。本明細書で使用するとき、一意識別子は、数字、文字、記号など、又はそれらの組合せの文字列であることが可能である。一意識別子は、所与のシステム内の単一のエンティティに関連付けられることができる。一意識別子は、エンティティがアクセスし対話することができるように、そのエンティティをアドレス指定又は識別するために用いることができる。本開示のいくつかの実施形態では、デバイスを他のエンティティと区別するために、一意識別子を、デバイス又はエンティティ、例えばスマートロック、モバイルデバイスなどに割り当てることができる。一意識別子は、デバイス（例えば送信端末）の媒体アクセス制御（ＭＡＣ）アドレス、ＩＰアドレス、特定のタグ、ユーザ名又はユーザＩＤなど、又はそれらの任意の組合せであることが可能である。

【００４５】

操作Ｓ１０３：送信端末は、操作命令又は予め設定されたルールに従って、送信すべきデータを生成し、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信

すべきデータを復号することで暗号化データを決定することができる。送信端末は、スマートドアロック又はモバイル端末を含むことができる。

【００４６】

予め設定された暗号化アルゴリズムは、対称アルゴリズム又は非対称アルゴリズムであることができる。対称アルゴリズムは、秘密キーアルゴリズムと呼ばれることもある。対称アルゴリズムは、データを暗号化及び復号するために同じキーを使用する暗号アルゴリズムであることが可能である。例示的な対称アルゴリズムは、アメリカ国防総省のデータ暗号化標準（ＤＥＳ）、トリプルＤＥＳ、国際データ暗号化アルゴリズム（ＩＤＥＡ）、高度暗号化標準（ＡＥＳ）などを含むことができる。非対称アルゴリズムは、公開キーアルゴリズムと呼ばれることもある。非対称アルゴリズムは、データを暗号化及び復号するために異なるキーを用いる暗号アルゴリズムである。例示的な非対称アルゴリズムは、リベストシャミアエーデルマン（ＲＳＡ）アルゴリズム、ディフィーヘルマンアルゴリズム、楕円曲線暗号（ＥＣＣ）アルゴリズム、デジタルシグネチャアルゴリズム（ＤＳＡ）アルゴリズムなどを含むことができる。

【００４７】

具体的には、スマートドアロックとモバイル端末は、同一の暗号化アルゴリズムで設定することができる。いくつかの実施形態では、スマートドアロックとモバイル端末は、暗号化アルゴリズムに対応する逆のアルゴリズムで設定することができる。暗号化及び復号は、スマートドアロックとモバイル端末内でローカルに行われて、エンドツーエンドの安全なデータ通信を実施することにより、情報漏洩のリスクを低減することができる。モバイル端末における組込み暗号化アルゴリズムは、モバイル端末に予めインストールされたスマートドアロックアプリによって実行することができる。

【００４８】

いくつかの実施形態では、送信端末は、モバイル端末又はスマートドアロックのうちの１つであることが可能である。送信端末は、モバイル端末を含み、受信端末は、スマートドアロックを含むことができる。送信端末は、スマートドアロックを含み、受信端末は、モバイル端末を含むことができる。送信端末と受信端末は、ユーザのニーズに応じて設定されてもよいが、これに限定されるものではない。送信端末は、操作命令又は予め設定されたルールに従って、送信すべきデータを生成し、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化することで暗号化データを決定することができる。動作命令は、データを要求する命令、又は、動作を行うよう要求する命令であり、本開示の例に示されるように、動作命令は、開錠パスワードを発行し、Ｂｌｕｅｔｏｏｔｈキーを要求し、遠隔で開錠し、パスワードを削除するなどのための命令である。予め設定されたルールは、すでに設定されているルールとして理解することができる。例えば、予め設定されたルールは、ロックが開錠されるたびに、１２時間ごとになどの予め設定された時間ルールであることが可能である。送信すべきデータは、スマートドアロックとモバイル端末との間で安全に送信する必要があるデータであることが可能である。いくつかの実施形態では、送信すべきデータは、スマートドアロックパスワード、Ｂｌｕｅｔｏｏｔｈキー、開錠記録、履歴、センサ状態など、又はそれらの任意の組合せであることが可能である。

【００４９】

送信すべきデータは、一般に、機密であり、セキュアな送信技術で送信する必要がある。そのため、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化して、暗号化データを取得することができる。このように、送信すべきデータは、暗号文の形式により、スマートドアロックとモバイル端末との間で送信することができる。

【００５０】

例えば、訪問者Ａがただ今スマートドアロックを開錠して住宅に入たい場合、ユーザは、予めインストールされたスマートドアロックアプリを用いてクラウドサーバを介してスマートドアロックに開錠パスワードを発行することができる。モバイル端末は送信端末と

して動作し、スマートドアロックは受信端末として動作することができる。モバイル端末は、開錠パスワードを送信すべきデータとして設定し、予め設定された暗号化アルゴリズムにより、送信すべきデータを暗号化して、暗号化データを決定することができる。

【００５１】

又は、モバイル端末は、予めインストールされたスマートドアロックアプリによりクラウドサーバを介して開錠のためのキーを発行する要求をスマートドアロックに送信することができる。モバイル端末は受信端末として動作し、スマートドアロックは送信端末として動作することができる。モバイル端末から送信された命令、例えばＢｌｕｅｔｏｏｔｈキーに対する要求が受信した場合、スマートドアロックは、その指示に従って対応するＢｌｕｅｔｏｏｔｈキーを送信すべきデータとして生成し、予め設定された暗号化アルゴリズムにより、送信すべきデータを処理することで暗号化データを決定することができる。

【００５２】

別の例として、モバイル端末は、予めインストールされたスマートドアロックアプリによりスマートドアロックに制御要求の命令を送信することができる。モバイル端末は送信端末として動作し、スマートドアロックは受信端末として機能することができる。例えば、モバイル端末からの制御要求の命令は、パスワード、Ｂｌｕｅｔｏｏｔｈキーなどを付加するよう制御すること、ロックを遠隔で開錠すること、パスワード、Ｂｌｕｅｔｏｏｔｈキー、指紋などを削除することを含むことができる。予め設定された暗号化アルゴリズムを用いて送信すべきデータを暗号化することで暗号化データを決定するように、命令を設定することができる。

【００５３】

本開示のいくつかの実施形態では、スマートドアロックは、送信端末として動作し、指定のデータ（例えば開錠記録、履歴記録、ドア上のセンサの状態、及び住宅にいる人の存在など）を、ユーザの予め設定されたルール（例えば、１２時間ごとに送信すること、各ドアの解錠の後にアップロードすること、定時的に送信することなど）に従って、指定のモバイル端末に送信することができる。即ち、スマートドアロックは、送信端末として動作し、予め設定された暗号化アルゴリズムにより、送信すべき解錠記録を暗号化して暗号化データを決定し、予め設定されたルール（例えば、１２時間ごとに送信すること、各ドアの解錠の後にアップロードすること、定時的に送信することなど）に従って、解錠記録を処理して暗号化データを決定することができる。

【００５４】

操作Ｓ１０４：送信端末は、暗号化データに一意識別子を割り当てることができる。

【００５５】

具体的には、送信端末は、暗号化データに一意識別子を割り当てることで、一意識別子付き暗号化データを決定することができる。一意識別子は、送信端末の識別情報を表し、認証において識別子照合を行うために用いられる。一意識別子は、例えば、送信端末のＭＡＣアドレス、ＩＰアドレス、特定のタグ、ユーザ名又はユーザＩＤなど、又はそれらの任意の組合せを含むことができる。

【００５６】

操作Ｓ１０５：送信端末は、一意識別子付き暗号化データを受信端末に送信することができる。

【００５７】

いくつかの実施形態では、送信端末は、予め設定された通信チャネルを介して、又はクラウドサーバにより、一意識別子付き暗号化データを受信端末に送信することができる。受信端末は、モバイル端末又はスマートドアロックであることが可能である。予め設定された通信チャネルは、短距離無線通信チャネル又はＮＦＣチャネルであることが可能であり、ＷｉＦｉローカルエリアネットワーク、Ｂｌｕｅｔｏｏｔｈチャネル、Ｚｉｇｂｅｅチャネル、又はＮＦＣチャネルのうちの１つを含むが、これらに限定されない。スマートロックシステムのローカル制御は、予め設定された通信チャネルを介して実行することができ、スマートロックシステムの遠隔制御は、クラウドサーバを介して実行することがで

きる。
【００５８】
例えば、訪問者Ａがただ今スマートドアロックを開錠して住宅に入たい場合、ユーザは、予めインストールされたスマートドアロックアプリを用いてクラウドサーバを介してスマートドアロックに開錠パスワードを発行することができる。モバイル端末は送信端末として動作し、スマートドアロックは受信端末として動作することができる。モバイル端末は、開錠パスワードを送信すべきデータとして設定し、予め設定された暗号化アルゴリズムにより、送信すべきデータを暗号化することで暗号化して暗号化データを決定し、暗号化データに一意識別子を割り当て、一意識別子付き暗号化データをクラウドサーバ又は予め設定された通信チャネルを介してスマートドアロックに送信することができる。
【００５９】
本開示のいくつかの実施形態では、スマートドアロックは、送信端末として動作し、指定のデータ（例えば開錠記録）を、ユーザの予め設定されたルール（例えば、１２時間ごとに送信すること）に従って、指定のモバイル端末に送信することができる。即ち、スマートドアロックは、送信端末として動作し、予め設定された暗号化アルゴリズムにより解錠記録を暗号化して暗号化データを決定し、予め設定されたルール（例えば、１２時間ごとに送信すること）に従って、解錠記録を処理して暗号化データを形成し、一意識別子を割り当て、一意識別子付き暗号化データをクラウドサーバ又は予め設定された通信チャネルを介してモバイル端末に送信することができる。
【００６０】
操作Ｓ１０６：受信端末は、一意識別子付き暗号化データに基づいて本人認証をすることができる。
【００６１】
具体的には、受信端末による一意識別子付き暗号化データに基づいて本人認証をすることは、以下のような動作を含むことができる。
【００６２】
操作Ｓ１０６１：受信端末は、一意識別子付き暗号化データ中の一意識別子を抽出することができる。
【００６３】
受信端末として、モバイル端末又はスマートドアロックは、一意識別子付き暗号化データの持っている一意識別子を抽出することができる。例えば、送信端末は、一意識別子付き暗号化データを送信し、受信端末は、一意識別子（例えば、抽出された一意識別子は、ＭＡＣアドレス、ＩＰアドレス、特定のタグ、ユーザ名、又は送信端末のユーザＩＤであることが可能である）。
【００６４】
操作Ｓ１０６２：一意識別子に基づいて一意識別子に対応する暗号化キーを決定する。
【００６５】
抽出された一意識別子に基づいて照合操作を行うことで、一意識別子に対応する暗号化キーを決定することができる。モバイル端末もスマートドアロックも、一意識別子と暗号化キーとの間の対応関係を記憶することができ、一意識別子の照合操作により、一意識別子に対応する暗号化キーを決定することができる。例えば、モバイル端末もスマートドアロックも、一意識別子と暗号化キーとの対応関係テーブルを記憶していることが可能である。一意識別子に基づいて照合検索を行うと、対応する暗号化キーを決定することができる。
【００６６】
操作Ｓ１０６３：一意識別子に対応する暗号化キーに基づいて認証の結果を決定する。
【００６７】
具体的には、受信端末は、照合操作によって決定された暗号化キーが、受信端末に記憶されている暗号化キーと同じであるか又は対応するかを判定することができる。それらが同じであるか又は互いに対応する場合、認証の結果は、暗号化データが対になっている送

信端末によって送信されたとすることができる。本明細書で使用するとき、対になっている送信端末は、検証された送信端末を表すことができる。それらが互いに異なるか又は対応しない場合、認証の結果は、暗号化データが対になっていない送信端末によって送信されたとすることができる。本明細書で使用するとき、対になっていない送信端末は、検証されていない送信端末を表すことができる。本開示では、認証操作を適用して、通信のセキュリティを保証し、強化することができる。

【００６８】

操作Ｓ１０７：受信端末は、本人認証の結果に応じて、暗号化データを処理することができる。受信端末は、モバイル端末又はスマートドアロックであることが可能である。

【００６９】

具体的には、本人認証の結果が、暗号化データが対になっている送信端末から送信されたとなる場合、復号及び更なる処理を行うことができる。本人認証の結果が、暗号化データが対になっていない送信端末から送信されたとなる場合、復号を行なわず、警報を生成することができる。

【００７０】

いくつかの実施形態では、警報は、例えば、テキストメッセージ、音声信号、光信号、振動、触覚警報など、又はそれらの組合せなど、任意の形態で提示することができる。警報は、サーバに更新するか、又は受信端末に記憶することができる。警告は、スマートドアロック、例えば警察署であるサードパーティー、セキュリティ監視エンティティなど、又はそれらの組み合わせと対になった別のモバイル端末に送信することができる。

【００７１】

本開示の方法はまた、以下の操作を含むことができる。

【００７２】

操作Ｓ１０１：ユーザの許可命令に応答して、スマートドアロック又はモバイル端末は、初期暗号化キーを生成し、初期暗号化キーを認証することで暗号化キーを決定することができる。

【００７３】

初期暗号化キーは、スマートドアロック又はモバイル端末によって自動的に生成されるか、又はユーザによって手動で入力されるキーであることが可能である。初期暗号化キーは、セキュア通信チャネルを介して送信することができる。このようにして、スマートドアロックもモバイル端末も、初期暗号化キーを取得することができる。スマートドアロックとモバイル端末は、初期暗号化キーを認証することで暗号化キーを決定することができる。

【００７４】

具体的には、例えば、ユーザが手動で設定ボタン又は設定モードタッチキーを押して、予め設定された管理者パスワードを入力するか又はローカルに管理者権限指紋をスマートドアロックに入力する（即ち、スマートドアロックが設定モードに入る）ことで、ユーザの許可指示を行うことができる。ユーザは、端末でアプリを開いて設定モードに入り、設定モードによりユーザの許可でセキュア通信チャネルを起動することができる。スマートドアロックとモバイル端末は、ＷｉＦｉＬＡＮネットワーク、Ｂｌｕｅｔｏｏｔｈチャネル、Ｚｉｇｂｅｅチャネル、又はＮＦＣチャネルのいずれか１つを用いたセキュア通信チャネルを介して接続することができる。初期暗号化キーは、スマートドアロック又はモバイル端末のいずれかによって生成することができ、暗号化キーは、スマートドアロックとモバイル端末によって相互に認証することで決定することができる。例えば、ユーザは、スマートドアロックの開始設定ボタンを押し、認証された管理者パスワードを入力するとともに、ユーザは、モバイル端末内のスマートドアロックアプリを開いて、設定モードに入ることができる。スマートドアロックと携帯電話は、ユーザの許可で、Ｂｌｕｅｔｏｏｔｈチャネルを介して接続して通信することができる。初期暗号化キーは、スマートドアロックによって生成し、Ｂｌｕｅｔｏｏｔｈ通信チャネルを介してモバイル端末内のスマートドアロックアプリに送信することができる。モバイル端末内のアプリは、初期暗号化

キーを確認又は修正し、スマートドアロックと交換することができる。あるいは、スマートドアロックとモバイル端末アプリは、それぞれ、一対の公開キーと秘密キーを生成して交換することができる。

【００７５】

いくつかの実施形態では、送信すべき暗号化データのために複数の実装形態がある。例えば、暗号化のために対称暗号化又は非対称暗号化を用いることができる。以下、異なる暗号化方法での暗号化及び復号化プロセスを、特定の実施形態を参照しながら詳細に説明する。

【００７６】

任意選択で、図３に示すように、暗号化キーは、第１の暗号化キーである。操作Ｓ１０３において、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを復号することで暗号化データを決定することは、以下のような動作を含むことができる。

【００７７】

操作Ｓ１０３１ａ：対称暗号化アルゴリズムを用いて第１の暗号化キーに基づいて送信すべきデータを暗号化することで初期暗号化データを決定する。

【００７８】

具体的には、第１の暗号化キーは、スマートドアロックとモバイル端末にそれぞれ記憶された暗号化キーであることが可能である。例えば、スマートドアロックが２つのモバイル端末と対になっている場合、モバイル端末Ａとスマートドアロックは、同じ暗号化キー（例えばキーＡ）を記憶することができる。モバイル端末Ｂとスマートドアロックは、同じ暗号化キー（例えばキーＢ）を記憶することができる。いくつかの実施形態では、モバイル端末Ａを送信端末として使用する場合、暗号化アルゴリズムを用いて暗号化キー「キーＡ」に基づいて、モバイル端末Ａによって生成された送信すべきデータを暗号化することで、初期暗号化データＡを決定することができる。いくつかの実施形態では、スマートドアロックを送信端末として使用し、暗号化アルゴリズムを用いて暗号化キー「キーＢ」に基づいて、モバイル端末Ｂによって送信された命令に従って生成された送信すべきデータを暗号化することで、初期暗号化データＢを決定することができる。

【００７９】

操作Ｓ１０３２ａ：初期暗号化データに対して予め設定されたキー値を設定する。

【００８０】

具体的には、上記の操作により決定された初期暗号化データに対して、タイムスタンプ、カウンタ値、ランダムコードの少なくとも１つである、予め設定されたキー値を設定することができる。タイムスタンプは、現在のタイムスタンプ（例えば、関心のある操作（例えば、データの暗号化、ドアを解除するようとの要求）が行われた日付及び／又は時刻）であることができる。例えば、現在の時間が２０１６－０８－１１－２０：２１である場合、これを予め設定されたキー値として用いて、初期暗号化データに設定することができる。

【００８１】

操作Ｓ１０３３ａ：予め設定されたキー値で設定された初期暗号化データに検証署名を付加することで、暗号化データを決定する。

【００８２】

検証署名は、ハッシュアルゴリズムより生成されたハッシュ値であることが可能で、検証署名は、復号時に暗号化データの完全性を検証するために使用することができる。

【００８３】

任意選択で、図４に示すように、操作Ｓ１０７において、本人認証の結果に応じて暗号化データを処理することは、以下の操作を含むことができる。

【００８４】

動作Ｓ１０７１ａにおいて、本人認証の結果が一致である場合、受信端末は、暗号化データの検証署名を検証することができる。本明細書で使用するとき、一致であるという本

人認証の結果は、暗号化データが、対になっている又は他の信頼できる送信端末から送信されたことを示すことができる。照合操作によって決定された暗号化データの暗号化キーは、受信端末に記憶されている暗号化キーと同じであってもよく、対応していてもよい。

【００８５】

具体的には、受信端末は、検証署名の完全性を検証して、データの改ざんを防止し、データの完全性を保証することができる。

【００８６】

動作Ｓ１０７１ａにおいて、署名検証の結果が一致である場合、受信端末は、予め設定されたキー値が正当であるかを検証することができる。本明細書で使用するとき、一致である検証署名は、暗号化データが、対になっている又は他の信頼できる送信端末から送信されたことを示すことができる。暗号化データの検証署名は、受信端末によって決定された値と一致することができる。この値は、タイムスタンプ、カウンタ値、又はランダムコードなどであってもよい。

【００８７】

具体的には、検証署名が一致する場合、受信端末は、予め設定されたキー値（例えば、タイムスタンプ、カウンタ値、又はランダムコード）が正当であるかを分析することができる。具体的には、予め設定されたキー値を、受信端末内のローカルなデータと比較することができ、ローカルデータは、受信端末によって記憶又は生成することができる。いくつかの実施形態では、スマートドアロックが受信端末として動作する場合、スマートドアロックは、タイムスタンプをスマートドアロックのクロックモジュールに記憶された時刻データと比較することができる。時計モジュールは、ボタン電池で連続的に電力供給される時計チップを含むことができる。例えば、スマートドアロックは、単三乾電池で電力供給することができる。電池を変更する操作は、スマートドアロック内部の時計の通常動作を中断しない。時計モジュールは、標準時間に従って自動的に更新することができる。例えば、現在の時刻は１７：００であり、時計モジュールの時刻も１７：００である。

【００８８】

スマートロックは、タイムスタンプを、スマートドアロックの時計モジュールに記憶された時刻と比較することができる。偏差（即ち、暗号化データのタイムスタンプと時計モジュールに記憶された時刻との差）が閾値を超える場合、暗号化データは不正なデータパッケージであると見なすことができる。検証結果を、Ｂｌｕｅｔｏｏｔｈ、ＺｉｇＢｅｅなどを介してモバイル端末にフィードバックすることができる。一般に、閾値は、場合に応じて１５分～６０分以内に設定し、例えば、閾値を２０分とすることができる。偏差が２０分を超える場合、暗号化データは不正なデータパッケージであると見なすことができる。検証結果は、予め設定されたキー値を備える暗号化データが不正であるとなり、予め設定された通信チャネル又はクラウドサーバを介して、検証結果を、モバイル端末にフィードバックすることができる。

【００８９】

偏差が閾値を超えていない場合、検証結果は、予め設定されたキー値を備える暗号化データが正当であるとすることができる。同様に、モバイル端末が受信端末として動作する場合、モバイル端末の現在の時刻値と比較することができるが、ここで、詳細な説明は省略する。

【００９０】

いくつかの実施形態では、予め設定されたキー値は、カウンタ値であることが可能である。スマートドアロックが受信端末として動作する場合、スマートドアロックは、予め設定されたキー値で設定された暗号化データのカウンタ値を、ローカルに記憶されたカウンタ値と比較することができる。カウンタ値は、暗号化キーに対応する複数の開錠時刻の表示であることができる。

【００９１】

暗号化データのカウンタ値がローカルに記憶されたカウンタ値よりも大きい場合、検証結果は、該カウンタ値を備える開錠検証コードが正当であることとすることができる。暗

号化データのカウンタ値がローカルに記憶されたカウンタ値以下である場合、暗号化データのデータパケットがリプレイされたと理解することができる。照合結果は、カウンタ値を備える暗号化データが不正であるとなり、予め設定された通信チャネル又はクラウドサーバを介して、検証結果を、モバイル端末にフィードバックすることができる。モバイル端末は、受信端末と同様に動作することができ、詳細はここでは説明しない。

【００９２】

操作Ｓ１０７３ａにおいて、予め設定されたキー値が正当である場合、受信端末は、対称暗号化アルゴリズムの逆のアルゴリズムを用いて第１の暗号化キーに基づいて、初期暗号化データを復号することで送信すべきデータを決定することができる。

【００９３】

具体的には、受信端末は、予め設定されたキー値で設定される暗号化データの予め設定されたキーが正当であるかを検証することができる。予め設定されたキー値が正当である場合、受信端末は、対称暗号化アルゴリズムの逆のアルゴリズムを用いて受信端末にローカルに記憶された第１の暗号化キーに基づいて、初期暗号化データを復号することで送信すべきデータを決定することができる。例えば、ローカルに記憶された対応する第１の暗号化キーが、「キーＡ」である場合、送信すべきデータは、対称暗号化アルゴリズムの逆のアルゴリズムを用いて「キーＡ」に基づいて初期暗号化データを復号することで取得することができる。

【００９４】

任意選択で、暗号化キーは、公開キーと秘密キーを含むことができる。操作Ｓ１０３において、予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化することで暗号化データを決定することは、以下のような動作を含むことができる。

【００９５】

操作Ｓ１０１ｂ：送信端末は、非対照暗号化アルゴリズムを用いて送信端末に記憶された公開キーに基づいて送信すべきデータを暗号化することで初期暗号化データを決定することができる。

【００９６】

具体的には、送信端末と受信端末にそれぞれ記憶された暗号化キーは、公開キーと秘密キーを含むことができる。送信端末によって記憶された暗号化キーは、秘密キーｐｒｉ－Ａと公開キーｐｕｂ－Ｂを含むことができる。同時に、受信端末によって記憶された対応する暗号化キーは、秘密キーｐｒｉ－Ｂと公開キーｐｕｂ－Ａを含むことができる。例えば、送信端末として動作するスマートドアロックによって記憶された暗号化キーは、秘密キーｐｒｉ－Ａと公開キーｐｕｂ－Ｂを含み、受信端末として動作するモバイル端末によって記憶された対応する暗号化キーは、秘密キーｐｒｉ－Ｂと公開キーｐｕｂ－Ａを含むことができる。送信端末として動作するスマートドアロックは、非対称暗号化アルゴリズムを用いて、自身に記憶された公開キーｐｕｂ－Ｂに基づいて、送信すべきデータを暗号化することで初期暗号化データを決定することができる。

【００９７】

操作Ｓ１０３２ｂ：初期暗号化データに対して予め設定されたキー値を設定すること。予め設定されたキー値は、タイムスタンプ、カウンタ値、又はランダムコードのうちの少なくとも１つであることが可能である。タイムスタンプは、現在のタイムスタンプ（例えば、関心のある操作が行われた日付及び／又は時刻）であることができる。

【００９８】

具体的には、上記の操作により決定された初期暗号化データに対して、タイムスタンプ（例えば現在のタイムスタンプ）、カウンタ値、ランダムコードの少なくとも１つである、予め設定されたキー値を設定することができる。例えば、現在の時間が２０１６－０８－１１－２０：２１である場合、タイムスタンプを予め設定されたキー値として設定し、初期暗号化データに設定することができる。

【００９９】

操作Ｓ１０３３ｂ：予め設定されたキー値で設定された初期暗号化データに、送信端末に記憶された秘密キーである検証署名を付加することで、暗号化データを決定すること。

【０１００】

具体的には、以上説明したように、送信端末によって記憶された暗号化キーは、秘密キーｐｒｉ－Ａと公開キーｐｕｂ－Ｂを含むことができる。同時に、受信端末によって記憶された対応する暗号化キーは、秘密キーｐｒｉ－Ｂと公開キーｐｕｂ－Ａを含むことができる。例えば、送信端末としてのスマートドアロックによって記憶された暗号化キーは、秘密キーｐｒｉ－Ａと公開キーｐｕｂ－Ｂを含み、受信端末としてのモバイル端末によって記憶された対応する暗号化キーは、秘密キーｐｒｉ－Ｂと公開キーｐｕｂ－Ａを含むことができる。例えば、スマートドアロックが送信端末として動作する場合、予め設定されたキー値を備える初期暗号化データに検証署名を付加することで決定することができ、検証署名は、スマートドアロックに記憶された秘密キーｐｒｉ－Ａであることが可能である。

【０１０１】

任意選択で、操作Ｓ１０７において、本人認証の結果に応じて暗号化データを処理することは、以下の操作を含むことができる。

【０１０２】

動作Ｓ１０７１ｂにおいて、本人認証の結果が一致である場合、受信端末は、受信端末によって記憶された公開キーを用いて、暗号化データの検証署名を検証することができる。本明細書で使用するとき、一致であるという本人認証の結果は、暗号化データが、対になっている又は他の信頼できる送信端末から送信されたことを示すことができる。照合操作によって決定された暗号化データの暗号化キーは、受信端末に記憶されている暗号化キーと同じであってもよく、対応していてもよい。

【０１０３】

具体的には、本人認証の結果が一致である場合、受信端末は、受信端末にローカルに記憶された公開キーを用いて、暗号化データの検証署名を検証することができる。例えば、受信端末は、モバイル端末であることが可能である。以上説明したように、モバイル端末内にローカルに記憶された暗号化キーは、秘密キーｐｒｉ－Ｂと公開キーｐｕｂ－Ａを含むことができる。また、モバイル端末は、ローカルに記憶された公開キーｐｕｂ－Ａを用いて、暗号化データ内で持っている検証署名ｐｒｉ－Ａを検証することができる。ｐｒｉ－Ａがローカルに記憶された公開キーｐｕｂ－Ａに対応すると検証された場合、検証署名は一致する。ローカルに記憶された公開キーｐｕｂ－Ａに対応する秘密キーではないと検証された場合、検証署名の結果は不一致となる。

【０１０４】

操作Ｓ１０７２ｂ：署名検証の結果が一致である場合、受信端末は、予め設定されたキー値が正当であるかを検証する。本明細書で使用するとき、一致である検証署名は、暗号化データが、対になっている又は他の信頼できる送信端末から送信されたことを示すことができる。暗号化データの検証署名は、受信端末によって決定された値と一致することができる。この値は、タイムスタンプ、カウンタ値、又はランダムコードなどであってもよい。

【０１０５】

具体的には、検証署名の結果が一致である場合、受信端末は、予め設定されたキー値（例えば、タイムスタンプ、カウンタ値、又はランダムコード）が正当であるかを分析することができる。具体的には、予め設定されたキー値を、受信端末内のローカルなデータと比較することができ、ローカルデータは、受信端末によって記憶又は生成することができる。いくつかの実施形態では、スマートドアロックが受信端末として動作する場合、スマートドアロックは、タイムスタンプをスマートドアロックのクロックモジュールに記憶された時刻データと比較することができる。クロックモジュールは、電池で連続的に電力供給される時計チップを含むことができる。例えば、スマートドアロックは、単三乾電池で電力供給することができる。電池を変更する操作は、ドアロック内部の時計の通常動作を中断しない。時計モジュールは、標準時間に従って自動的に更新することができる。例え

ば、現在の時刻は１７：００であり、時計モジュールの時刻も１７：００である。
【０１０６】
スマートロックは、タイムスタンプを、スマートドアロックの時計モジュールに記憶された時刻と比較することができる。偏差（即ち、暗号化データのタイムスタンプと時計モジュールに記憶された時刻との差）が閾値を超える場合、暗号化データは不正なデータパッケージであると見なすことができる。検証結果を、Ｂｌｕｅｔｏｏｔｈ、ＺｉｇＢｅｅなどを介してモバイル端末にフィードバックすることができる。一般に、閾値は、状況に応じて１５分～６０分以内に設定することができる。例えば、閾値を２０分とすることができる。偏差が２０分を超える場合、暗号化データが不正なデータパッケージを含むと見なすことができる。検証結果は、予め設定されたキー値を備える暗号化データが不正であるとなり、予め設定された通信チャネル又はクラウドサーバを介して、検証結果を、モバイル端末にフィードバックすることができる。
【０１０７】
偏差が閾値を超えていない場合、検証結果は、予め設定されたキー値を備える暗号化データが正当であるとなる。同様に、モバイル端末が受信端末として動作する場合、モバイル端末の現在の時間値に対する比較を行うことができるが、詳細はここでは省略する。
【０１０８】
いくつかの実施形態では、予め設定されたキー値は、カウンタ値であることが可能である。スマートドアロックが受信端末として動作する場合、スマートドアロックは、予め設定されたキー値で設定された暗号化データのカウンタ値を、ローカルに記憶されたカウンタ値と比較することができる。
【０１０９】
暗号化データのカウンタ値がローカルに記憶されたカウンタ値よりも大きい場合、検証結果は、該カウンタ値を備える開錠検証コードが正当であることとすることができる。暗号化データのカウンタ値がローカルに記憶されたカウンタ値以下である場合、暗号化データのデータパケットがリプレイされたと理解することができる。照合結果は、カウンタ値を備える暗号化データが不正であるとなり、予め設定された通信チャネル又はクラウドサーバを介して、検証結果を、モバイル端末にフィードバックすることができる。モバイル端末は、受信端末と同じであってもよく、詳細はここでは省略する。
【０１１０】
操作Ｓ１０７３ｂ：予め設定されたキー値が正当である場合、受信端末は、同じ対称暗号化アルゴリズムの逆のアルゴリズムを用いて自身に記憶された秘密キーに基づいて初期暗号化データを復号することで送信すべきデータを決定することができる。
【０１１１】
不正な人によるデータ改ざんを防止し、データの完全性を保証するために、送信すべきデータを暗号化し、予め設定されたキー値を付加してリプレイを防止し、認証署名を設定するなどのことがローカルに行うため、サーバ又はスマートドアロック製造業者の内部職員であっても、誰でもサーバからユーザの送信すべき情報を取得できない。従って、サーバが侵害された場合であっても、ドアロックとモバイル端末との間の通信における本人認証、アンチリプレイ及び改ざん防止が有効に保ち、ユーザ情報の安全を効果的に保護することができる。
【０１１２】
操作Ｓ１０７１ａ～Ｓ１０７３ａ及び操作Ｓ１０７１ｂ～Ｓ１０７３ｂは、受信端末によって暗号化データを復号するいくつかの特定の実施形態である。本開示のいくつかの実施形態では、受信端末は、送信端末によって送信された一意識別子付き暗号化データを受信し、一意識別子付き暗号化データに対して本人認証を行うことで本人認証の結果を決定することができる。受信端末は、本人認証の結果に応じて、キー交換プロセスにより取得した暗号化キーに基づいて、暗号化データを復号することで、送信すべきデータを取得することができる。暗号化データの暗号化方式によっては、暗号化データを復号する方式が異なることが可能である。本開示の実施形態はこれを限定するものではない。

【０１１３】
ユーザが自分のモバイル端末を紛失した場合、バックアップモバイル端末にログインするで、関連する暗号化キーの情報を削除するようスマートドアロック及び／又はクラウドサーバに命令するために、削除操作を依然として起動できる。これにより、紛失したモバイル端末内の暗号化キー情報の漏洩を防止し、セキュリティリスクを低減することができる。
【０１１４】
任意選択で、スマートドアロックシステムに基づくセキュア通信方法は、以下の操作をさらに含むことができる。
【０１１５】
操作１０８１：モバイル端末のバックアップデバイスであるバックアップモバイル端末は、ユーザの本人性を検証するための情報であるアカウントログイン検証情報を取得することができる。本明細書で使用するとき、モバイル端末のバックアップデバイスは、ユーザによって選択された任意のデバイスであることが可能である。
【０１１６】
本開示のいくつかの実施形態では、ユーザがアプリを予めインストールされて暗号化キーを記憶したモバイル端末を紛失した場合、ユーザは、スマートドアロックアプリが予めインストールされたバックアップモバイル端末により、アカウントログイン検証情報を入力することでログインすることができる。アカウントログイン検証情報は、ユーザ識別情報（ユーザ名、ユーザＩＤなどの、ユーザがルールに従って設定したユーザ識別情報）、パスワード、検証コードなどを含むが、これらに限定されない。
【０１１７】
操作１０８２：アカウントログイン検証情報が検証された場合、バックアップモバイル端末は、ユーザによる削除操作の許可に応答して、スマートドアロックに第１の削除命令を送信して、そのローカルに記憶された暗号化キー情報を削除するようスマートドアロックに命令し、及び／又は、バックアップモバイル端末は、ユーザによる削除操作の遠隔許可に応答して、クラウドサーバに第２の削除命令を送信して、モバイル端末に記憶された暗号化キー情報を削除するようクラウドサーバに命令することができる。
【０１１８】
具体的には、アカウントログイン検証がパスした後、ユーザの端末デバイスは、短距離無線通信又はＮＦＣ接続を介してスマートドアロックに接続し、スマートロックを制御して、アカウントに対応する元の暗号化キー情報を削除することができる。同時に、紛失したモバイル端末に記憶された暗号化キーは、クラウドサーバを介して行われるいくつかの操作によって削除することができる。
【０１１９】
上記の説明は、本開示で提供されるセキュア通信方法のいくつかの実施形態である。理解しやすくするために、以下、特定の場面において、本開示の実施形態を説明する。実施形態１は、モバイル端末が送信端末として動作し、開錠パスワードをスマートドアロックに送信して開錠を実施する応用場面である。実施形態２は、スマートドアロックが送信端末として動作し、開錠レコード、センサ状態などを予め設定されたルールに従って指定のモバイル端末に送信する応用場面である。以下、実施するプロセスについて詳細に説明する。
【実施例１】
【０１２０】
スマートドアロックシステムに適用可能なセキュア通信方法であって、以下の操作を含む。
【０１２１】
（１）ユーザの許可命令に応答して、スマートドアロックとモバイル端末は、それぞれ、セキュア通信チャネルを起動することができる。
【０１２２】

セキュア通信チャネルは、スマートドアロックとモバイル端末の許可によって起動される通信チャネルである。

【０１２３】

スマートドアロック又はモバイル端末は、スマートドアロック又はモバイル端末は、初期暗号化キーを生成し、初期暗号化キーを認証することで暗号化キーを決定することができ、初期暗号化キーは、スマートドアロック又はモバイル端末によって自動的に生成されるか、又はユーザによって手動で入力されるキーであることが可能である。

【０１２４】

具体的には、ユーザの許可指示は、例えば、ユーザが手動で設定ボタン又は設定モードタッチキーを押して、予め設定された管理者パスワードを入力するか又はローカルに管理者権限指紋をスマートドアロックに入力する（即ち、スマートドアロックが設定モードに入る）ことであることが可能である。ユーザは、モバイル端末内のアプリを開いて設定モードに入り、設定モードによりユーザの許可でセキュア通信チャネルを起動することができる。スマートドアロックとモバイル端末は、ＷｉＦｉＬＡＮ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＺｉｇＢｅｅ、又はＮＦＣのいずれか１つを用いたセキュア通信チャネルを介して接続することができる。初期暗号化キーは、スマートドアロック又はモバイル端末のいずれかによって生成することができ、暗号化キーは、スマートドアロックとモバイル端末によって相互に認証することで決定することができる。例えば、ユーザは、スマートドアロックの開始設定ボタンを押し、認証された管理者パスワードを入力するとともに、ユーザは、モバイル端末内のスマートドアロックアプリを開いて、設定モードに入ることができる。スマートドアロックと携帯電話は、ユーザの許可で、Ｂｌｕｅｔｏｏｔｈチャネルを介して接続することができる。初期暗号化キーは、スマートドアロックによって生成し、Ｂｌｕｅｔｏｏｔｈ通信チャネルを介して携帯電話内のスマートドアロックアプリに送信することができる。携帯電話内のアプリは、初期暗号化キーを確認又は修正し、スマートドアロックと交換することができる。あるいは、スマートドアロックと携帯電話アプリは、それぞれ、一対の公開キーと秘密キーを生成して交換することができる。

【０１２５】

（２）スマートドアロックとモバイル端末は、Ｂｌｕｅｔｏｏｔｈ通信を起動し、スマートドアロックと、モバイル端末に予めインストールされたスマートドアロックアプリとは、暗号化キーをＢｌｕｅｔｏｏｔｈ通信により交換することができる。

【０１２６】

（３）モバイル端末を送信端末として用いる場合、モバイル端末に予め設定されたスマートドアロックアプリの開錠パスワードに応じて、送信すべきデータを生成することができる。予め設定された暗号化アルゴリズムを用いて暗号化キーに基づいて送信すべきデータを暗号化することで、暗号化データを決定することができる。具体的には、スマートドアロックと、モバイル端末に予めインストールされたスマートドアロックアプリには、同じ暗号化キー「キーＡ」と同じ対称暗号化アルゴリズムが組込まれている。また、モバイル端末を受信端末として用い、スマートドアロックを受信端末として用いることができる。モバイル端末は、送信すべきデータとしてパスワードを設定した後、暗号化アルゴリズムを用いて暗号化キー「キーＡ」に基づいて、送信すべきデータを暗号化することで、初期暗号化データＡを決定することができる。タイムスタンプである予め設定されたキー値を用いて初期暗号化データＡを設定することができる。予め設定されたキー値で設定された初期暗号化データに検証署名を付加することで、暗号化データを決定することができる。

【０１２７】

（４）モバイル端末は、暗号化データに一意識別子を割り当てることができる。一意識別子は、スマートドアロックアプリが予め設定されたモバイル端末のユーザＩＤであることができる。

【０１２８】

（５）モバイル端末は、クラウドサーバを介して一意識別子付き暗号化データをスマートドアロックに送信することができる。

【０１２９】
（６）暗号化データを受信するスマートドアロックは、一意識別子付き暗号化データに対して本人性検証を行うことができる。具体的には、受信端末として動作するスマートドアロックは、一意識別子付き暗号化データから一意識別子を抽出することができる。例えば、送信端末は、一意識別子を備える暗号化データを送信し、受信端末は、一意識別子（例えば、送信端末のＭＡＣアドレス、ＩＰアドレス、特定のタグ、ユーザ名、又はユーザＩＤなど）を抽出することができる。照合操作により、一意識別子に対応する暗号化キーを決定することができる。マートドアロックもモバイル端末も、一意識別子と暗号化キーとの対応関係を記憶することができる。対応関係に基づいて一意識別子の照合により、一意識別子に対応する暗号化キーを決定することができる。例えば、モバイル端末もスマートドアロックも、一意識別子と暗号化キーとの対応関係テーブルを記憶していることが可能である。一意識別子により照合検索を行うと、対応する暗号化キーを決定するができる。受信端末によって、一意識別子に対応する暗号化キー応じて、本人認証の結果を決定され得る。具体的には、受信端末は、照合において決定された暗号化キーが、受信端末に記憶されている暗号化キーと同じであるか又は対応するか否かを決定することができる。同じであるか又は一致する場合、本人認証の結果は、暗号化データが対になっている送信端末によって送信されたこととすることができる。同じでない又は一致しない場合、本人認証の結果は、暗号化データが対になっていない送信端末によって送信されたこととすることができる。本人認証操作により、通信の安全性を向上させることができる。

【０１３０】
（７）本人認証の結果が一致である場合、受信端末は、暗号化データの検証署名を検証することができる。受信端末は、署名の完全性を検証して、改ざんを防止し、データの完全性を保証することができる。具体的には、署名検証の結果が一致である場合、スマートドアロックは、タイムスタンプをスマートドアロック内の時計モジュールによって記憶された時刻と比較することができる。時計モジュール内の時計チップは、ボタン電池で連続的に電力供給することができる。例えば、スマートドアロックは、単三乾電池で電力供給することができる。単三電池を交換した後でも、ドアロック内の時計は正確に運転し続ける。時計モジュールの時間は、標準時間に従って自動的に更新することができる。例えば、現在の時刻は１７：００であり、時計モジュールの時刻も１７：００である。

【０１３１】
スマートロックは、タイムスタンプを、スマートドアロックの時計モジュールに記憶された時刻と比較することができる。偏差（即ち、暗号化データのタイムスタンプと時計モジュールに記憶された時刻との差）が閾値を超える場合、暗号化データは不正なデータパッケージであると決定することができる。検証結果を、Ｂｌｕｅｔｏｏｔｈ、ＺｉｇＢｅなどを介してモバイル端末にフィードバックすることができる。一般に、閾値は、場合に応じて１５分～６０分以内に設定し、例えば、閾値を２０分とすることができる。偏差が２０分を超える場合、暗号化データが不正なデータパッケージであると決定することができる。検証結果は、予め設定されたキー値を備える暗号化データが不正であるとなり、予め設定された通信チャネル又はクラウドサーバを介して、検証結果を、モバイル端末にフィードバックすることができる。

【０１３２】
偏差が閾値を超えていない場合、検証結果は、予め設定されたキー値を備える暗号化データが正当であるとすることができる。予め設定されたキー値が正当である場合、スマートロックは、同じ対称暗号化アルゴリズムの逆のアルゴリズムを用いて、ローカルに記憶された同じ第１の暗号化キー「キーＡ」に基づいて、初期暗号化データを復号することで、送信すべきデータを決定することができる。

【実施例２】

【０１３３】
スマートドアロックシステムによるセキュア通信方法であって、以下の操作を含む。

【０１３４】

（１）ユーザの許可命令に応答して、スマートドアロックとモバイル端末は、それぞれ、セキュア通信チャネルを起動することができ、セキュア通信チャネルは、スマートドアロックとモバイル端末の許可によって起動される通信チャネルである。

【０１３５】

スマートドアロック又はモバイル端末は、初期暗号化キーを生成することができ、スマートドアロックとモバイル端末は、初期暗号化キーを認証することで暗号化キーを決定することができる。初期暗号化キーは、スマートドアロック又はモバイル端末によって自動的に生成されるか、又はユーザによって手動で入力されるキーであることが可能である。

【０１３６】

具体的には、ユーザの許可指示は、例えば、ユーザが手動で設定ボタン又は設定モードタッチキーを押して、予め設定された管理者パスワードを入力するか又はローカルに管理者権限指紋をスマートドアロックに入力する（即ち、スマートドアロックが設定モードに入る）ことであることが可能である。ユーザは、モバイル端末内のアプリを開いて設定モードに入り、設定モードによりユーザの許可でセキュア通信チャネルをトリガすることができる。スマートドアロックとモバイル端末は、ＷｉＦｉＬＡＮネットワーク、Ｂｌｕｅｔｏｏｔｈチャネル、Ｚｉｇｂｅｅチャネル、又はＮＦＣチャネルのいずれか１つを用いたセキュア通信チャネルを介して接続することができる。スマートドアロック又はモバイル端末のいずれかによって初期暗号化キーを生成し、スマートドアロックとモバイル端末が相互に認証することで、暗号化キーを決定することができる。例えば、ユーザは、スマートドアロックの開始設定ボタンを押し、認証された管理者パスワードを入力するとともに、ユーザは、モバイル端末内のスマートドアロックアプリを開いて、設定モードに入ることができる。スマートドアロックと携帯電話は、ユーザの許可で、ＮＦＣチャネルを介して接続することができる。スマートドアロックと携帯電話アプリは、それぞれ、対になっている公開キーと秘密キーを生成し、ＮＦＣチャネルを介してそれらを交換することができる。

【０１３７】

（２）スマートドアロックと、モバイル端末に予めインストールされたスマートドアロックアプリとは、暗号化キーをＮＦＣチャネルを介して交換することができる。

【０１３８】

（３）スマートドアロックを送信端末として用いる場合、例えば、指定のデータ（例えば、開錠記録、履歴記録、ドアのセンサの状態、及び住宅にいる人の存在など）を、ユーザの予め設定されたルール（例えば、１２時間ごとに送信すること、各ドアの解錠の後にアップロードすること、定時的に送信することなど）に従って、指定のモバイル端末に送信することができる。即ち、スマートドアロックは、送信端末として機能して、予め設定された暗号化アルゴリズムを用いて送信すべき開錠レコードを暗号化することで暗号化データを決定することができる。具体的には、送信端末としてのスマートドアロックによって記憶された暗号化キーは、秘密キーｐｒｉ－Ａ、公開キーｐｕｂ－Ｂ及び非対称暗号化アルゴリズムを含み、受信端末としてのモバイル端末によって記憶された対応する暗号化キーは、秘密キーｐｒｉ－Ｂ、公開ｐｕｂ－Ａ及び同じ非対称暗号化アルゴリズムを含むことができる。スマートドアロックは、送信端末として動作して、非対称暗号化アルゴリズムを用いて自身に記憶された公開キーｐｕｂ－Ｂに基づいて送信すべきデータを暗号化して初期暗号化データを決定し、予め設定されたキー値としてカウンタ値を用いて初期暗号化データを設定して、予め設定されたキー値で設定された初期暗号化データを決定し、秘密キーを検証署名として、予め設定されたキー値で設定された初期暗号化データに付加して暗号化データを決定することができる。具体的には、以上説明したように、送信端末によって記憶された暗号化キーは、秘密キーｐｒｉ－Ａと公開キーｐｕｂ－Ｂを含むことができる。また、受信端末に記憶された対応する暗号化キーは、秘密キーｐｕｂ－Ｂと公開キーｐｕｂ－Ａを含むことができる。例えば、送信端末としてのスマートドアロックによって記憶された暗号化キーは、秘密キーｐｒｉ－Ａと公開キーｐｕｂ－Ｂを含み、受信端末としてのモバイル端末によって記憶された対応する暗号化キーは、秘密キーｐｒｉ－

Ｂと公開キーｐｕｂ－Ａを含むことができる。スマートドアロックが送信端末として用いられる場合、予め設定されたキー値を備える初期暗号化データに検証署名を付加することで決定することができ、検証署名は、スマートドアロックによって記憶された秘密キーｐｒｉ－Ａであることが可能である。

【０１３９】

（４）スマートドアロックは、暗号化データに対して一意識別子を設定することができる。一意識別子は、スマートドアロックのＭＡＣアドレスであることができる。

【０１４０】

（５）スマートドアロックは、クラウドサーバを介して一意識別子付き暗号化データをモバイル端末に送信することができる。

【０１４１】

（６）データを受信するモバイル端末は、一意識別子付き暗号化データに対して本人性検証を行うことができる。具体的には、スマートドアロックは、受信端末として用いられ、暗号化データ内の一意識別子を抽出することができる。例えば、送信端末は、一意識別子を備える暗号化データを送信し、受信端末は、一意識別子（例えば、送信端末のＭＡＣアドレス、ＩＰアドレス、特定のタグ、ユーザ名、又はユーザＩＤなど）を抽出することができる。受信端末は、抽出された一意識別子に基づいて一意識別子の照合を行うことで、一意識別子に対応する暗号化キーを決定することができる。モバイル端末もスマートドアロックも、一意識別子と暗号化キーとの間の対応関係を記憶することができ、一意識別子の照合により、一意識別子に対応する暗号化キーを決定することができる。例えば、モバイル端末もスマートドアロックも、一意識別子と暗号化キーとの対応関係テーブルを記憶していることが可能である。一意識別子により照合検索を行うと、対応する暗号化キーを決定するができる。受信端末は、一意識別子に対応する暗号化キーにより、本人認証の結果を決定することができる。具体的には、受信端末は、照合において決定された暗号化キーが、受信端末に記憶されている暗号化キーと同じであるか又は対応するか否かを決定することができる。同じであるか又は一致する場合、本人認証の結果は、暗号化データが対になっている送信端末によって送信されたこととすることができる。同じでない又は一致しない場合、本人認証の結果は、暗号化データが対になっていない送信端末によって送信されたこととすることができる。本人認証操作により、通信の安全性を向上させることができる。

【０１４２】

（７）本人認証の結果が一致である場合、受信端末は、記憶された公開キーに基づいて暗号化データの検証署名を検証することができる。具体的には、本人性検証の結果が一致である場合、受信端末は、ローカルに記憶された公開キーに基づいて暗号化データの検証署名を検証することができる。例えば、受信端末は、モバイル端末であることが可能である。以上説明したように、モバイル端末内にローカルに記憶された暗号化キーは、秘密キーｐｒｉ－Ｂと公開キーｐｕｂ－Ａを含むことができる。また、モバイル端末は、ローカルに記憶されたｐｕｂ－Ａを用いて、暗号化データ内で持っている署名ｐｒｉ－Ａを検証することができる。ローカルに記憶された公開キーｐｕｂ－Ａに対応する秘密キーｐｒｉ－Ａであると検証された場合、検証署名は一致である。ローカルに記憶された公開キーｐｕｂ－Ａに対応する秘密キーではないと検証された場合、検証署名の結果は不一致となる。署名検証の結果が一致であれば、モバイル端末が受信端末として用いられる場合、モバイル端末は、予め設定されたキー値で設定された暗号化データのカウンタ値を、ローカルに記憶されたカウンタ値と比較することができる。

【０１４３】

暗号化データのカウンタ値がローカルに記憶されたカウンタ値よりも大きい場合、検証結果は、該カウンタ値を備える開錠検証コードが正当であることとすることができる。暗号化データのカウンタ値がローカルに記憶された値以下である場合、データパケットがリプレイされると理解することができる。照合結果は、カウンタ値を備える暗号化データが不正であるとなり、予め設定された通信チャネル又はクラウドサーバを介して、検証結果

を、スマートドアロックにフィードバックして、警報情報を生成することができる。予め設定されたキー値が正当である場合、受信端末は、同じ対称暗号化アルゴリズムの逆のアルゴリズムを用いて秘密キーに基づいて初期暗号化データを復号することで送信すべきデータを決定することができる。本開示のシリアル番号は、専ら例示を目的として、実施形態の利点及び欠点を表すものではない。

【０１４４】

本開示の上記の実施形態において、様々な実施形態の説明にはそれぞれ重点があり、詳細は、一実施形態において詳細に説明されていないものは、他の実施形態の関連する説明を参照することができる。

【０１４５】

本開示のいくつかの実施形態において開示された技術内容は、他の方式で実施するできることを理解すべきである。上述した装置の実施形態は模式的なもののみであり、例えば、ユニットの分割は、論理的な機能分割であってもよく、実際に実施する場合、実際には他の分割態様を有していてもよい。例えば、複数のユニット又は構成要素が組み合せても、別のシステムに統合してもよく、一部の特徴を省略するか又は実行しなくてもよい。また、図示又は説明された相互結合又は直接結合又は通信接続は、いくつかのインターフェース、ユニット又はモジュールを介した間接的な結合又は通信接続であってもよく、電気的又は別の方法で行ってもよい。

【０１４６】

別個の構成要素として説明されたユニットは、物理的に別個であってもなくてもよく、ユニットとして示された構成要素は、物理的ユニットであってもなくてもよく、例えば、１つの場所に配置されてもよく、又は複数のユニットに分散されてもよい。実際の需要に応じて、一部又は全部のユニットで実施形態の解決策の目的を達成することができる。

【０１４７】

また、本開示の各実施形態における各機能部は、１つの処理部に統合してもよく、各単独のユニットの物理的なユニットであってもよく、２以上のユニットが一体化されてもよい。統合されたユニットは、ハードウェアの形態で、又はソフトウェア機能ユニットの形態で実施することができる。

【０１４８】

上記の説明は、本開示の好ましい実施形態にすぎず、当業者が本開示の原理から逸脱することなく、改善及び修正を行い得ることに留意されたい。これらの改善及び修正も、本開示の範囲に属すると理解すべきである。

【図面】

【図１】

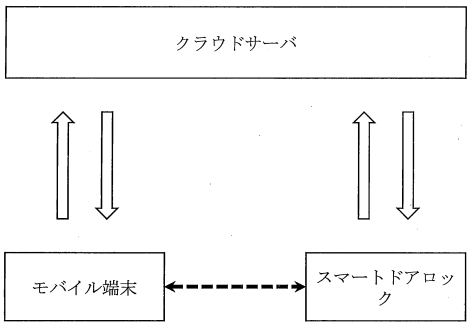

図１

【図２】

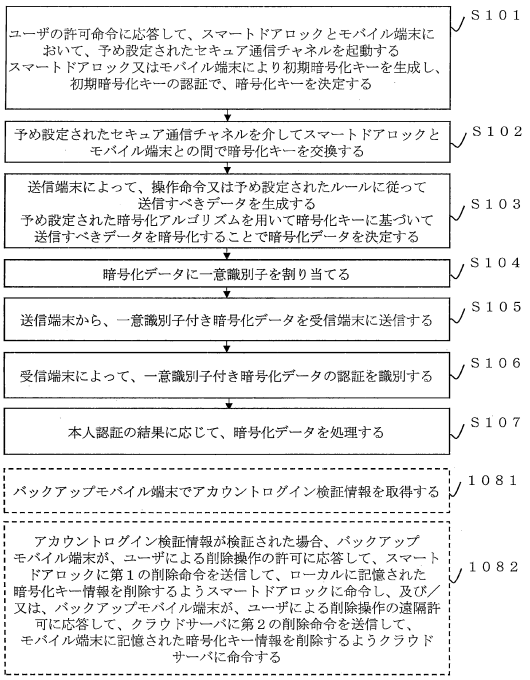

図２

【図３】

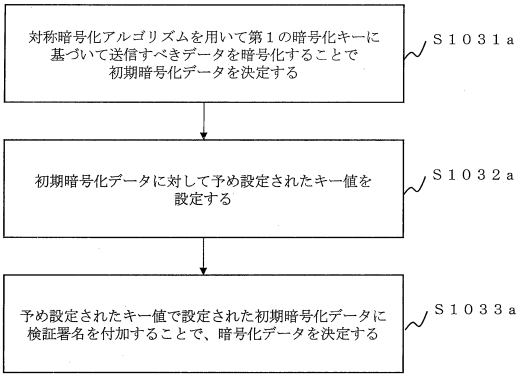

図３

【図４】

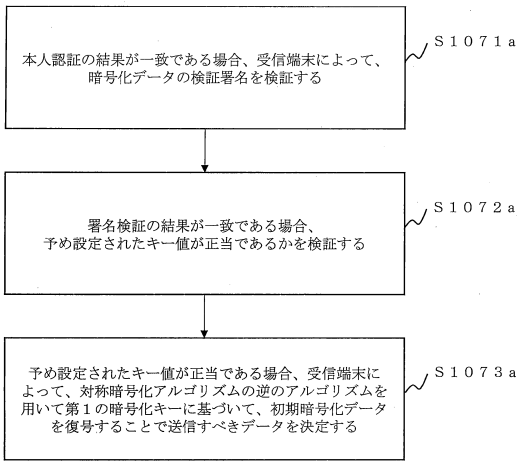

図４

フロントページの続き

(74)代理人　100133400
弁理士　阿部 達彦
(72)発明者　▲唐▼ 皓
中華人民共和国１０２２０８北京市昌平区回▲龍▼▲観▼▲東▼大街３８８号 回▲龍▼▲観▼▲創▼客▲廣▼▲場▼エー座５▲層▼

審査官　中里 裕正
(56)参考文献　特表２０１７－５０５２５３（ＪＰ，Ａ）
特開２００９－２１２７３２（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｅ０５Ｂ　４９／００
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　９／０８
Ｇ０６Ｆ　２１／３１
Ｈ０４Ｗ　１２／０６