【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和2年8月6日(2020.8.6)

【公表番号】特表2019-519176(P2019-519176A)
【公表日】令和1年7月4日(2019.7.4)
【年通号数】公開・登録公報2019-026
【出願番号】特願2018-567679(P2018-567679)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/16　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｈ０４Ｌ　9/00　６４３
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】令和2年6月23日(2020.6.23)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
鍵管理方法であって、
暗号解読能力を有するシステムにおいて、各エンティティの鍵の組が該エンティティの秘密暗号鍵と該エンティティの該秘密暗号鍵に対応する偽の秘密鍵とを有する、前記エンティティの複数の鍵の組をエンティティから遠隔に保管するステップと、
前記エンティティから暗号文コンテンツ及び偽の秘密鍵を受け取るステップと、
前記暗号文コンテンツが特定のエンティティについて前記秘密暗号鍵を用いて暗号解読されている時に、前記特定のエンティティの前記偽の秘密鍵に基づいて前記特定のエンティティについての遠隔に保管された前記鍵の組から前記エンティティの前記秘密暗号鍵を取得するステップと、
を含むことを特徴とする方法。
【請求項２】
前記暗号要素が、前記特定のエンティティの新たな秘密鍵と、前記特定のエンティティの前記新たな秘密鍵に対応する偽の秘密鍵とを生成するステップと、
前記暗号要素が、前記偽の秘密鍵を前記特定のエンティティに送信するステップと、
をさらに含む、請求項１に記載の方法。
【請求項３】
前記エンティティの前記新たな秘密鍵を用いて前記暗号文コンテンツを暗号解読するステップをさらに含み、
前記特定のエンティティの前記偽の秘密鍵は、前記特定のエンティティの新たな秘密鍵へのポインタをさらに含むものである、請求項２に記載の方法。
【請求項４】
前記特定のエンティティの前記秘密鍵を取得するステップは、前記暗号要素のユニフォームリソースロケータを鍵情報から抽出するステップと、前記暗号要素の前記ユニフォー

ムリソースロケータと前記偽の秘密鍵とに基づいて前記特定のエンティティの前記新たな秘密鍵を取り出すステップとをさらに含む、
請求項１に記載の方法。
【請求項５】
各エンティティは、暗号解読能力を有するアプリケーション、暗号解読能力を有する装置、及び暗号解読能力を有するアプリケーションを使用するユーザのうちの１つである、
請求項１に記載の方法。
【請求項６】
鍵管理システムであって、
それぞれが自身の秘密暗号鍵と鍵ストレージとを用いた公開鍵暗号解読能力を有する１又は２以上のエンティティと、
特定のエンティティの新たな秘密暗号鍵と、該新たな秘密暗号鍵に対応する偽の秘密鍵とを生成するメタデータエンコーダを有する、コンピュータネットワークによって前記エンティティに接続された暗号要素と、
を備え、前記暗号要素は、前記特定のエンティティに前記偽の秘密鍵を送信する、
ことを特徴とするシステム。
【請求項７】
前記暗号要素は、前記特定のクライアントからの暗号文と前記偽の秘密鍵とを含む要求に基づいて暗号解読プロセスを実行し、前記暗号要素は、前記偽の秘密鍵に基づいて前記特定のエンティティの前記新たな秘密鍵を取得して、前記特定のエンティティの前記新たな秘密鍵を用いた前記暗号文の前記暗号解読を可能にする、
請求項６に記載のシステム。
【請求項８】
各エンティティは、前記特定のエンティティの前記新たな秘密鍵を用いた前記暗号文の前記暗号解読を実行する暗号解読モジュールを有し、
前記暗号解読モジュールは、鍵情報を受け取る構文解析器モジュール、及び前記偽の秘密鍵に基づいて前記特定のエンティティの前記新たな秘密鍵を取得するメタ情報抽出器モジュール、をさらに含む、
請求項７に記載のシステム。
【請求項９】
前記メタ情報抽出器モジュールは、前記鍵情報から前記暗号要素のユニフォームリソースロケータを抽出し、該暗号要素の該ユニフォームリソースロケータに基づいて前記特定のエンティティの前記新たな秘密鍵を取り出す、
請求項８に記載のシステム。
【請求項１０】
各エンティティは、暗号解読能力を有するアプリケーション、暗号解読能力を有する装置、及び暗号解読能力を有するアプリケーションを使用するユーザのうちの１つである、
請求項６に記載のシステム。
【請求項１１】
前記特定のエンティティの前記偽の秘密鍵は、前記特定のエンティティの新たな秘密鍵へのポインタをさらに含む、
請求項６に記載のシステム。
【請求項１２】
鍵管理方法であって、
エンティティに送信される暗号文を暗号解読する前記エンティティの秘密暗号鍵を生成するステップと、
前記生成した秘密暗号鍵を、前記エンティティから離れた、鍵ストレージを有する鍵管理要素に保管するステップと、
鍵管理要素において、前記秘密暗号鍵を使用して、前記生成された秘密暗号鍵へのポインタとしての役割を果たす偽の秘密鍵を生成するステップと、

前記偽の秘密鍵を前記エンティティに送信して鍵ストレージに保管するステップと、
を含み、前記エンティティは、前記偽の秘密鍵を用いて要求を行うことによって暗号文を暗号解読する、
ことを特徴とする方法。
【請求項１３】
新たなエンティティである前記エンティティの公開鍵を生成するステップをさらに含み、
エンティティの前記秘密鍵を生成するステップは、既存のエンティティの新たな秘密鍵を生成するステップをさらに含む、
請求項１２に記載の方法。
【請求項１４】
前記エンティティは、暗号解読能力を有するアプリケーション、暗号解読能力を有する装置、及び暗号解読能力を有するアプリケーションを使用するユーザのうちの１つである、
請求項１２に記載の方法。
【請求項１５】
前記特定のエンティティの前記偽の秘密鍵は、前記特定のエンティティの新たな秘密鍵へのポインタをさらに含む、
請求項１２に記載の方法。