【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3年8月19日(2021.8.19)

【公表番号】特表2020-529758(P2020-529758A)
【公表日】令和2年10月8日(2020.10.8)
【年通号数】公開・登録公報2020-041
【出願番号】特願2020-502218(P2020-502218)
【国際特許分類】
Ｈ０４Ｌ　9/16　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６４３
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】令和3年7月6日(2021.7.6)
【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】
データを暗号化及び復号する方法であって、前記方法は埋め込みシステムによって実行され、
前記埋め込みシステムの真の乱数の生成器によって、複数の鍵を生成すること、
前記埋め込みシステムの鍵メモリ内に前記複数の鍵を書き込むこと、及び
前記鍵メモリからの前記複数の鍵のうちの少なくとも１つの鍵を使用して暗号化及び復号操作を行うことであって、前記少なくとも１つの鍵が、前記埋め込みシステムのデータメモリに書き込まれる取得データを暗号化し、前記データメモリから読み取られる暗号化データを復号するために使用されること
を含む、方法。
【請求項２】
前記複数の鍵を生成することが、
前記データメモリ内のデータを分けるかどうかを判断すること、及び
前記判断に応答して暗号化及び復号操作を行うこと
を更に含む、請求項１に記載の方法。
【請求項３】
前記判断に応答して暗号化及び復号操作を行うことが、
前記データメモリ内の前記データを分けると判断することに応答して、
　前記データメモリを複数の論理データ記憶域に分割すること、及び
　前記複数の論理データ記憶域のデータに対して暗号化及び復号操作を選択的に行うこと
を含む、請求項２に記載の方法。
【請求項４】
前記複数の論理データ記憶域のデータに対して前記暗号化及び復号操作を選択的に行うことが、前記複数の論理データ記憶域のうちの第１の論理データ記憶域に対して第１の鍵を使用し、前記複数の論理データ記憶域のうちの第２の論理データ記憶域に対して第２の鍵を使用する、請求項３に記載の方法。

【請求項５】
前記第１の鍵が前記第２の鍵と異なる、請求項４に記載の方法。
【請求項６】
前記第１の鍵及び前記第２の鍵が、別のデータメモリに関連付けられた別の鍵と異なる、請求項４に記載の方法。
【請求項７】
前記判断に応答して暗号化及び復号操作を行うことが、
前記データメモリ内の前記データを分けないと判断することに応答して、全データ記憶域のデータに対して暗号化及び復号操作を行うこと
を含む、請求項２に記載の方法。
【請求項８】
前記全データ記憶域のデータに対して前記暗号化及び復号操作を行うことが、前記全データ記憶域に対して統一鍵を使用する、請求項７に記載の方法。
【請求項９】
前記全データ記憶域に対する前記統一鍵が、別のデータメモリに関連付けられた別の鍵と異なる、請求項８に記載の方法。
【請求項１０】
前記暗号化及び復号操作を行うことが、単一サイクルの暗号化及び復号アルゴリズムを使用する、請求項１に記載の方法。
【請求項１１】
前記暗号化及び復号アルゴリズムが、排他的ＯＲ暗号化又はシーケンス再構成の一方を含む、請求項１０に記載の方法。
【請求項１２】
前記複数の鍵のうちの前記少なくとも１つの鍵が、前記埋め込みシステムの始動時に前記鍵メモリによって自動で取得される、請求項１に記載の方法。
【請求項１３】
前記データメモリ及び前記鍵メモリが、前記埋め込みシステムの同じ物理媒体上に位置する、請求項１に記載の方法。
【請求項１４】
前記埋め込みシステムが攻撃されているとの判断に応答して、前記鍵メモリ内に記憶されている前記複数の鍵をクリアすることを更に含む、請求項１に記載の方法。
【請求項１５】
データを暗号化及び復号する埋め込みシステムであって、
複数の鍵を生成するように構成される真の乱数の生成器と、
前記複数の鍵を記憶するように構成される鍵メモリを含むメモリバンクと、
前記鍵メモリからの前記複数の鍵のうちの少なくとも１つの鍵を使用して暗号化及び復号操作を行うように構成されるメモリモジュールであって、前記少なくとも１つの鍵が、前記埋め込みシステムのデータメモリに書き込まれる取得データを暗号化し、前記データメモリから読み取られる暗号化データを復号するために使用される、メモリモジュールとを含む、システム。
【請求項１６】
前記メモリモジュールが、
前記データメモリ内のデータを分けるかどうかを判断し、
前記判断に応答して、暗号化及び復号操作を行う
ように更に構成される、請求項１５に記載のシステム。
【請求項１７】
前記メモリモジュールが、
前記データメモリ内の前記データを分けると判断することに応答して、
　前記データメモリを複数の論理データ記憶域に分割し、
　前記複数の論理データ記憶域のデータに対して暗号化及び復号操作を選択的に行う

ように更に構成される、請求項１６に記載のシステム。
【請求項１８】
前記メモリモジュールが、前記複数の論理データ記憶域のうちの第１の論理データ記憶域に対して第１の鍵を使用し、前記複数の論理データ記憶域のうちの第２の論理データ記憶域に対して第２の鍵を使用するように更に構成される、請求項１７に記載のシステム。
【請求項１９】
前記第１の鍵が前記第２の鍵と異なる、請求項１８に記載のシステム。
【請求項２０】
前記第１の鍵及び前記第２の鍵が、別のデータメモリに関連付けられた別の鍵と異なる、請求項１８に記載のシステム。
【請求項２１】
前記メモリモジュールが、
前記データメモリ内の前記データを分けないと判断することに応答して、全データ記憶域のデータに対して暗号化及び復号操作を行う
ように更に構成される、請求項１６に記載のシステム。
【請求項２２】
前記メモリモジュールが、前記全データ記憶域に対して統一鍵を使用するように更に構成される、請求項２１に記載のシステム。
【請求項２３】
前記メモリモジュールが、前記暗号化及び復号操作を行うために、単一サイクルの暗号化及び復号アルゴリズムを使用するように構成される、請求項２２に記載のシステム。
【請求項２４】
前記暗号化及び復号アルゴリズムが、排他的ＯＲ暗号化又はシーケンス再構成の一方を含む、請求項２３に記載のシステム。
【請求項２５】
前記複数の鍵のうちの前記少なくとも１つの鍵が、前記埋め込みシステムの始動時に前記鍵メモリによって自動で取得される、請求項１５に記載のシステム。
【請求項２６】
前記データメモリ及び前記鍵メモリが、前記埋め込みシステムの同じ物理媒体上に位置する、請求項１５に記載のシステム。
【請求項２７】
前記メモリモジュールが、前記埋め込みシステムが攻撃されているとの判断に応答して、前記鍵メモリ内に記憶されている前記複数の鍵をクリアするように更に構成される、請求項１５に記載のシステム。