【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6年3月25日(2024.3.25)

【国際公開番号】WO2023/199436
【出願番号】特願2024-504811(P2024-504811)
【国際特許分類】
H04L 9/16(2006.01)
【FI】
H04L 9/16

【手続補正書】
【提出日】令和6年1月25日(2024.1.25)
【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】
公開鍵及び第１復号可能条件を用いて公開鍵暗号方式の暗号化を実行することによって、第１変換後公開鍵暗号文と、前記第１変換後公開鍵暗号文に対応する鍵とを生成する変換先設定部と、
第２共通鍵暗号秘密鍵を平文とし、前記第１変換後公開鍵暗号文に対応する鍵を秘密鍵として共通鍵暗号方式の暗号化を実行することによって第１部分変換鍵を生成し、
第１共通鍵暗号秘密鍵及び第１補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値と、前記第２共通鍵暗号秘密鍵及び第２補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値との排他的論理和を、第２部分変換鍵として算出する鍵生成部と
を備える変換鍵生成装置と、
前記第１共通鍵暗号秘密鍵及び前記第１補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値及び平文の排他的論理和である共通鍵暗号文と、前記第２部分変換鍵との排他的論理和を、前記共通鍵暗号文を生成する際に用いた平文を復号することに用いられる変換後共通鍵暗号文の少なくとも一部として算出する変換部
を備える変換装置と
を備える暗号文変換システム。
【請求項２】
前記変換後共通鍵暗号文は、前記変換後共通鍵暗号文の少なくとも一部と、前記第２補助情報とから成る請求項１に記載の暗号文変換システム。
【請求項３】
前記公開鍵暗号方式は、属性ベース暗号方式である請求項１又は２に記載の暗号文変換システム。
【請求項４】
前記変換部は、前記公開鍵と、前記第１変換後公開鍵暗号文と、前記第１復号可能条件よりも限定的な条件である第２復号可能条件とを用いて属性ベース暗号方式の委譲変換を実行することにより第２変換後公開鍵暗号文を生成する請求項３に記載の暗号文変換システム。
【請求項５】
前記暗号文変換システムは、さらに、

前記第１復号可能条件に対応するユーザ秘密鍵と、前記第２変換後公開鍵暗号文とを用いて属性ベース暗号の復号を実行することによって前記第１変換後公開鍵暗号文に対応する鍵を復号し、
復号した前記第１変換後公開鍵暗号文に対応する鍵と、前記第１部分変換鍵とを用いて共通鍵暗号の復号を実行することによって前記第２共通鍵暗号秘密鍵を復号し、
前記変換後共通鍵暗号文の少なくとも一部と、復号した前記第２共通鍵暗号秘密鍵及び前記第２補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値との排他的論理和を、前記平文として算出する復号部
を備える復号装置
を備える請求項４に記載の暗号文変換システム。

【請求項６】
コンピュータである変換鍵生成装置が、公開鍵及び第１復号可能条件を用いて公開鍵暗号方式の暗号化を実行することによって、第１変換後公開鍵暗号文と、前記第１変換後公開鍵暗号文に対応する鍵とを生成し、
前記変換鍵生成装置が、第２共通鍵暗号秘密鍵を平文とし、前記第１変換後公開鍵暗号文に対応する鍵を秘密鍵として共通鍵暗号方式の暗号化を実行することによって第１部分変換鍵を生成し、
前記変換鍵生成装置が、第１共通鍵暗号秘密鍵及び第１補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値と、前記第２共通鍵暗号秘密鍵及び第２補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値との排他的論理和を、第２部分変換鍵として算出し、
コンピュータである変換装置が、前記第１共通鍵暗号秘密鍵及び前記第１補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値及び平文の排他的論理和である共通鍵暗号文と、前記第２部分変換鍵との排他的論理和を、前記共通鍵暗号文を生成する際に用いた平文を復号することに用いられる変換後共通鍵暗号文の少なくとも一部として算出する暗号文変換方法。

【請求項７】
公開鍵及び第１復号可能条件を用いて公開鍵暗号方式の暗号化を実行することによって、第１変換後公開鍵暗号文と、前記第１変換後公開鍵暗号文に対応する鍵とを生成する変換先設定処理と、
第２共通鍵暗号秘密鍵を平文とし、前記第１変換後公開鍵暗号文に対応する鍵を秘密鍵として共通鍵暗号方式の暗号化を実行することによって第１部分変換鍵を生成し、
第１共通鍵暗号秘密鍵及び第１補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値と、前記第２共通鍵暗号秘密鍵及び第２補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値との排他的論理和を、第２部分変換鍵として算出する鍵生成処理と
をコンピュータである変換鍵生成装置に実行させ、
前記第１共通鍵暗号秘密鍵及び前記第１補助情報を用いてブロック暗号のカウンターモードの暗号化を実行することによって算出した値及び平文の排他的論理和である共通鍵暗号文と、前記第２部分変換鍵との排他的論理和を、前記共通鍵暗号文を生成する際に用いた平文を復号することに用いられる変換後共通鍵暗号文の少なくとも一部として算出する変換処理
をコンピュータである変換装置に実行させる暗号文変換プログラム。