【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６部門第２区分
【発行日】平成23年2月17日(2011.2.17)

【公開番号】特開2009-175167(P2009-175167A)
【公開日】平成21年8月6日(2009.8.6)
【年通号数】公開・登録公報2009-031
【出願番号】特願2008-10548(P2008-10548)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６１０Ａ

【手続補正書】
【提出日】平成22年12月27日(2010.12.27)
【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】
データ変換装置であり、
ラウンド演算を繰り返すデータ変換処理を行なうデータ変換部を有し、
前記データ変換部は、
前記ラウンド演算において、
同一サイズのデータブロックを配列した長方形配列データを２分割した分割データの一方に対する線形変換処理と、
２つの分割データ相互の排他的論理和演算処理と、
分割データの一方のデータに対するシフト処理と、
２つの分割データのスワップ処理を実行する構成であるデータ変換装置。
【請求項２】
前記同一サイズのデータブロックは１バイト単位のデータブロックであり、前記データ変換部は、前記ラウンド演算において、１バイト単位のデータブロックを配列した長方形配列データを２分割した分割データに対する処理を行う構成である請求項１に記載のデータ変換装置。
【請求項３】
前記データ変換部は、
前記ラウンド演算において、さらに、
前記分割データの一方に対する非線形変換処理と、
前記分割データの一方に対する鍵適用演算処理を実行する構成である請求項１に記載のデータ変換装置。
【請求項４】
前記鍵適用演算は、前記分割データの一方の構成データと暗号鍵データとの排他的論理和演算である請求項３に記載のデータ変換装置。
【請求項５】
前記データ変換部は、
前記排他的論理和演算の結果を前記分割データの一方の更新データとして設定する請求項１に記載のデータ変換装置。
【請求項６】

前記データ変換部は、
前記シフト処理の実行に際して、
ｍ行２ｎ列の長方形配列データ中、シフト処理対象となるｍ行ｎ列の分割データが、ｍ≦ｎである場合、シフト前に同じ列のデータブロックがシフト処理後に異なる列になるようにシフトし、ｍ＞ｎの場合には、シフト前に同じ列のデータブロックがシフト処理後の任意の列に（ｍ／ｎ）－１個以上、（ｍ／ｎ）＋１個以下の範囲内で含まれるようにシフト処理を実行する請求項１に記載のデータ変換装置。
【請求項７】
前記データ変換部は、
前記シフト処理を２分割した分割データの双方に対して実行する請求項１に記載のデータ変換装置。
【請求項８】
前記データ変換部は、
前記ラウンド演算において、
前記分割データの一方の分割データＡに対して非線形変換処理と、シフト処理を実行して分割データＡの更新を行い、さらに更新された分割データＡに対する線形変換処理を実行して他方の分割データＢとの排他的論理和を実行して、その結果を分割データＢの更新データとして設定し、さらに分割データＡＢのスワップ処理の後、分割データＡに対する鍵データとの排他的論理和処理を実行する請求項１に記載のデータ変換装置。
【請求項９】
前記データ変換部は、
前記ラウンド演算において、
前記分割データの一方の分割データＡに対して非線形変換処理と、シフト処理を実行し、さらに線形変換処理を実行して分割データＡの更新を行い、さらに、更新された分割データＡと、他方の分割データＢとの排他的論理和を実行して、その結果を分割データＢの更新データとして設定し、さらに分割データＡＢのスワップ処理の後、分割データＡに対する鍵データとの排他的論理和処理を実行する請求項１に記載のデータ変換装置。
【請求項１０】
前記データ変換部は、
前記ラウンド演算において、
前記分割データの一方の分割データＡに対して非線形変換処理と、線形変換処理を実行して他方の分割データＢとの排他的論理和を実行して、その結果を分割データＢの更新データとして設定し、さらに分割データＡＢのスワップ処理の後、分割データＡに対するシフト処理と鍵データとの排他的論理和処理を実行する請求項１に記載のデータ変換装置。
【請求項１１】
前記データ変換部は、
前記ラウンド演算において、
前記分割データの一方の分割データＡに対して非線形変換処理と、シフト処理と線形変換処理を実行し、さらに、他方の分割データＢとの排他的論理和を実行して、その結果を分割データＡの更新データとして設定し、さらに分割データＡＢのスワップ処理の後、分割データＡに対する鍵データとの排他的論理和処理を実行する請求項１に記載のデータ変換装置。
【請求項１２】
前記データ変換部は、
前記ラウンド演算における線形変換処理において、複数の異なる行列をラウンド単位で選択適用する構成である請求項１に記載のデータ変換装置。
【請求項１３】
前記データ変換部は、
複数の異なる行列の選択適用としてＤＳＭ（Ｄｉｆｆｕｓｉｏｎ　Ｓｗｉｔｃｈｉｎｇ　Ｍｅｃｈａｎｉｓｍ）を利用した処理を行う構成である請求項１２に記載のデータ変換

装置。
【請求項１４】
データ変換装置において実行するデータ変換方法であり、
データ変換部が、ラウンド演算を繰り返してデータ変換を行なうデータ変換ステップを有し、
前記データ変換ステップは、
前記ラウンド演算において、
同一サイズのデータブロックを配列した長方形配列データを２分割した分割データの一方に対する線形変換処理と、
２つの分割データ相互の排他的論理和演算処理と、
分割データの一方のデータに対するシフト処理と、
２つの分割データのスワップ処理を実行するデータ変換方法。
【請求項１５】
前記同一サイズのデータブロックは１バイト単位のデータブロックであり、前記データ変換部は、前記ラウンド演算において、１バイト単位のデータブロックを配列した長方形配列データを２分割した分割データに対する処理を行う構成である請求項１４に記載のデータ変換方法。
【請求項１６】
前記データ変換ステップは、
前記ラウンド演算において、さらに、
前記分割データの一方に対する非線形変換処理と、
前記分割データの一方に対する鍵適用演算処理を実行する構成である請求項１４に記載のデータ変換方法。
【請求項１７】
前記鍵適用演算は、前記分割データの一方の構成データと暗号鍵データとの排他的論理和演算である請求項１６に記載のデータ変換方法。
【請求項１８】
前記データ変換ステップは、
前記排他的論理和演算の結果を前記分割データの一方の更新データとして設定する請求項１４に記載のデータ変換方法。
【請求項１９】
データ変換装置においてデータ変換処理を実行させるコンピュータ・プログラムであり、
データ変換部に、ラウンド演算を繰り返してデータ変換を行なわせるデータ変換ステップを有し、
前記データ変換ステップは、
前記ラウンド演算において、
同一サイズのデータブロックを配列した長方形配列データを２分割した分割データの一方に対する線形変換処理と、
２つの分割データ相互の排他的論理和演算処理と、
分割データの一方のデータに対するシフト処理と、
２つの分割データのスワップ処理を実行するステップであるコンピュータ・プログラム。
【請求項２０】
プログラムを実行するプロセッサと、
前記プログラムを保持するメモリと、
ラウンド演算を繰り返すデータ変換処理を行なうデータ変換部を有し、
前記データ変換部は、
前記ラウンド演算において、
同一サイズのデータブロックを配列した長方形配列データを２分割した分割データの一

方に対する線形変換処理と、
２つの分割データ相互の排他的論理和演算処理と、
分割データの一方のデータに対するシフト処理と、
２つの分割データのスワップ処理を実行する構成である情報処理装置。