【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17年8月11日(2005.8.11)

【公開番号】特開2005-31471(P2005-31471A)
【公開日】平成17年2月3日(2005.2.3)
【年通号数】公開・登録公報2005-005
【出願番号】特願2003-271525(P2003-271525)
【国際特許分類第７版】
　Ｇ０９Ｃ　1/00
【ＦＩ】
　Ｇ０９Ｃ　1/00　　６１０Ｂ

【手続補正書】
【提出日】平成17年3月16日(2005.3.16)
【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】
　暗号処理装置であり、
　入力データのデータ処理を実行するデータ処理部と、
　前記データ処理部におけるデータ処理によって生成される中間データを構成するビットデータの反転データを生成する反転データ生成手段と、
　前記中間データに対応する非反転ビットデータおよび反転ビットデータを各々格納する複数のデータ記憶部と、
　を有することを特徴とする暗号処理装置。
【請求項２】
　暗号処理方法であり、
　入力データのデータ処理を実行するデータ処理ステップと、
　前記データ処理ステップにおけるデータ処理によって生成される中間データを構成するビットデータの反転データを生成する反転データ生成ステップと、
　前記中間データに対応する非反転ビットデータおよび反転ビットデータを、各々複数のデータ記憶部に格納するデータ記憶ステップと、
　を有することを特徴とする暗号処理方法。
【請求項３】
　前記暗号処理方法は、共通鍵暗号処理方式に従った暗号処理を実行する暗号処理方法であり、
　前記データ処理ステップは、複数段のデータ変換ステップを有し、
　前記中間データは、前記データ変換ステップ各段の出力データであることを特徴とする請求項2に記載の暗号処理方法。
【請求項４】
　前記データ記憶ステップは、
　前記中間データを構成するビットデータを全く反転することなく格納する第１データ記憶ステップと、
　前記中間データを構成するビットデータを全て反転して格納する第２データ記憶ステップとからなることを特徴とする請求項2に記載の暗号処理方法。
【請求項５】

前記データ記憶ステップは、
前記中間データを構成するビットデータについて、ビット単位で反転または非反転したデータを格納する第１データ記憶ステップと、
前記中間データを構成するビットデータについて、前記第１データ記憶ステップにおいて記憶部に格納されるビットデータのビット単位の反転データを格納する第２データ記憶ステップとからなることを特徴とする請求項２に記載の暗号処理方法。
【請求項６】
前記暗号処理方法は、
データ記憶部の格納データが反転データであり、データ処理に適用すべきデータである場合に、格納データの再反転処理を行い、前記データ処理ステップは、該再反転データに対するデータ処理を実行することを特徴とする請求項２に記載の暗号処理方法。
【請求項７】
前記暗号処理方法は、
前記複数のデータ記憶部に対するデータ格納処理におけるハミングウェイトの和を一定に保持するように、前記中間データの非反転データおよび反転データ格納処理を実行することを特徴とする請求項２に記載の暗号処理方法。