【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18年3月23日(2006.3.23)

【公開番号】特開2006-39000(P2006-39000A)
【公開日】平成18年2月9日(2006.2.9)
【年通号数】公開・登録公報2006-006
【出願番号】特願2004-215484(P2004-215484)
【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17年12月6日(2005.12.6)
【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】
暗号処理の中断、再開機能を有し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理装置であって、
処理対象データを格納するデータ格納メモリと、
転送された処理対象データに対して共通鍵暗号により暗号化処理を行う共通鍵暗号ブロックと、
上記データ格納メモリから処理すべき転送データを指示する情報であるディスクリプタに基づいて、上記データ格納メモリから上記共通鍵暗号ブロックへのデータ転送を制御するメモリアクセスコントローラと、
を備え、
上記ディスクリプタは、共通鍵暗号における暗号アルゴリズムと、暗号処理モードと、が指示可能なディスクリプタフォーマットを有する
暗号処理装置。
【請求項２】
上記共通鍵暗号ブロックは、各種暗号処理モードでの処理時に使用されるデータをセットする記憶手段と、次のブロック処理時に使用されることになるデータを自動生成して保持する記憶手段を有する
請求項１記載の暗号処理装置。
【請求項３】
処理すべきデータが中断処理の対象となる場合、上記ディスクリプタでは転送開始位置と転送サイズの指定に加えて、中断処理の指示を指定する
請求項１記載の暗号処理装置。
【請求項４】
処理すべきデータが暗号化の対象となる場合、上記ディスクリプタでは転送開始位置と転送サイズの指定に加えて、暗号化の指示を指定する
請求項１記載の暗号処理装置。
【請求項５】
処理すべきデータが再開処理の対象となる場合、上記ディスクリプタでは転送開始位置と転送サイズの指定に加えて、再開処理の指示を指定する

請求項１記載の暗号処理装置。
【請求項６】
暗号処理の中断、再開機能を有し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理装置であって、
処理対象データを格納するデータ格納メモリと、
転送された処理対象データのハッシュ処理を行うハッシュブロックと、
上記データ格納メモリから処理すべき転送データを指示する情報であるディスクリプタに基づいて、上記データ格納メモリから上記ハッシュブロックへのデータ転送を制御するメモリアクセスコントローラと、
を備え、
上記ディスクリプタは、ハッシュ演算におけるハッシュアルゴリズムと、ハッシュ処理の中断と、ハッシュ処理の再開と、が指示可能なディスクリプタフォーマットを有する
暗号処理装置。
【請求項７】
上記ハッシュブロックは、ハッシュ処理の中断処理時に演算途中結果を保持する記憶手段と、ハッシュ処理の再開処理時に演算途中結果をセットできる記憶手段を有する
請求項６記載の暗号処理装置。
【請求項８】
処理すべきデータを中断も再開も行わずに一括で処理する場合、上記ディスクリプタでは中断無し、再開無しを指定する
請求項６記載の暗号処理装置。
【請求項９】
処理すべきデータがハッシュ演算の最初で処理されかつハッシュ演算を途中で中断する場合、上記ディスクリプタでは中断有り、再開無しを指示する
請求項６記載の暗号処理装置。
【請求項１０】
処理すべきデータがハッシュ演算の途中で処理されかつハッシュ演算を途中で中断する場合、上記ディスクリプタでは中断有り、再開有りを指示する
請求項６記載の暗号処理装置。
【請求項１１】
処理すべきデータがハッシュ演算の途中で処理されかつハッシュ演算の最後のデータとなる場合、上記ディスクリプタでは中断無し、再開有りを指示する
請求項６記載の暗号処理装置。
【請求項１２】
暗号処理の中断、再開機能を有し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理装置であって、
処理対象データを格納するデータ格納メモリと、
転送された処理対象データに対して共通鍵暗号により暗号化処理を行う共通鍵暗号ブロックと、
転送された処理対象データのハッシュ処理を行うハッシュブロックと、
上記データ格納メモリから処理すべき転送データを指示する情報であるディスクリプタに基づいて、上記データ格納メモリから上記共通鍵暗号ブロックおよび上記ハッシュブロックへのデータ転送を制御するメモリアクセスコントローラと、
を備え、
上記ディスクリプタは、
上記共通鍵暗号ブロックへのデータ転送を指示するときには、上記共通鍵暗号における暗号アルゴリズムと、暗号処理モードと、が指示可能なディスクリプタフォーマットを有するとともに、
上記ハッシュブロックへのデータ転送を指示するときには、ハッシュ演算におけるハッシュアルゴリズムと、ハッシュ処理の中断と、ハッシュ処理の再開と、が指示可能なディ

スクリプタフォーマットを有する
暗号処理装置。
【請求項１３】
ディスクリプタに基づいてデータ格納メモリから処理すべき転送データを指示し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理方法であって、
上記ディスクリプタは、共通鍵暗号における暗号アルゴリズムと、暗号処理モードと、が指示可能なディスクリプタフォーマットを有する
暗号処理方法。
【請求項１４】
ディスクリプタに基づいてデータ格納メモリから処理すべき転送データを指示し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理方法であって、
上記ディスクリプタは、ハッシュ演算におけるハッシュアルゴリズムと、ハッシュ処理の中断と、ハッシュ処理の再開と、が指示可能なディスクリプタフォーマットを有する
暗号処理方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００６
【補正方法】変更
【補正の内容】
【０００６】
上記目的を達成するため、本発明の第１の観点は、暗号処理の中断、再開機能を有し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理装置であって、処理対象データを格納するデータ格納メモリと、転送された処理対象データに対して共通鍵暗号により暗号化処理を行う共通鍵暗号ブロックと、上記データ格納メモリから処理すべき転送データを指示する情報であるディスクリプタに基づいて、上記データ格納メモリから上記共通鍵暗号ブロックへのデータ転送を制御するメモリアクセスコントローラと、を備え、上記ディスクリプタは、共通鍵暗号における暗号アルゴリズムと、暗号処理モードと、が指示可能なディスクリプタフォーマットを有する。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
本発明の第２の観点は、暗号処理の中断、再開機能を有し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理装置であって、処理対象データを格納するデータ格納メモリと、転送された処理対象データのハッシュ処理を行うハッシュブロックと、上記データ格納メモリから処理すべき転送データを指示する情報であるディスクリプタに基づいて、上記データ格納メモリから上記ハッシュブロックへのデータ転送を制御するメモリアクセスコントローラと、を備え、上記ディスクリプタは、ハッシュ演算におけるハッシュアルゴリズムと、ハッシュ処理の中断と、ハッシュ処理の再開と、が指示可能なディスクリプタフォーマットを有する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】

本発明の第３の観点は、暗号処理の中断、再開機能を有し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理装置であって、処理対象データを格納するデータ格納メモリと、転送された処理対象データに対して共通鍵暗号により暗号化処理を行う共通鍵暗号ブロックと、転送された処理対象データのハッシュ処理を行うハッシュブロックと、上記データ格納メモリから処理すべき転送データを指示する情報であるディスクリプタに基づいて、上記データ格納メモリから上記共通鍵暗号ブロックおよび上記ハッシュブロックへのデータ転送を制御するメモリアクセスコントローラと、を備え、上記ディスクリプタは、上記共通鍵暗号ブロックへのデータ転送を指示するときには、上記共通鍵暗号における暗号アルゴリズムと、暗号処理モードと、が指示可能なディスクリプタフォーマットを有するとともに、上記ハッシュブロックへのデータ転送を指示するときには、ハッシュ演算におけるハッシュアルゴリズムと、ハッシュ処理の中断と、ハッシュ処理の再開と、が指示可能なディスクリプタフォーマットを有する。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
本発明の第４の観点は、ディスクリプタに基づいてデータ格納メモリから処理すべき転送データを指示し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理方法であって、上記ディスクリプタは、共通鍵暗号における暗号アルゴリズムと、暗号処理モードと、が指示可能なディスクリプタフォーマットを有する。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】
本発明の第５の観点は、ディスクリプタに基づいてデータ格納メモリから処理すべき転送データを指示し、暗号処理に伴うパケット処理を一時中断して優先順位の高いパケットを先に処理する暗号処理方法であって、上記ディスクリプタは、ハッシュ演算におけるハッシュアルゴリズムと、ハッシュ処理の中断と、ハッシュ処理の再開と、が指示可能なディスクリプタフォーマットを有する。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
本発明によれば、ディスクリプタに基づいて、データ格納メモリから処理すべき転送データを指示するが、この情報となる各ディスクリプタは、共通鍵暗号の暗号アルゴリズムや暗号処理モードを指示可能なフィールドを含むディスクリプタフォーマットを有する。
このようなフォーマットを設けることにより、データ格納メモリに格納された全ての処理対象データのうち、たとえばDES-CBCモードで処理を行なう必要がある処理対象データに対しては、転送データ位置と転送データサイズとDESとCBCモードの指示を、またたとえば、AES-Counter Modeで処理を行なう必要がある処理対象データに対しては、転送データ位置と転送データサイズとAESとCounter Modeの指示を、それぞれの処理対象データに対して指示できる。
また、次のブロック処理時に使用されるデータを自動生成して保持することにより、処

理の中断時にはそのデータをストアし、処理の再開時にはストアしたデータをセットすることができ、これにより、処理の再開が容易に行われる。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】
また、本発明によれば、同様に、各ディスクリプタには、ハッシュアルゴリズムやハッシュ処理の中断やハッシュ処理の再開を指示可能なフィールドを含むものを、ディスクリプタフォーマットとして有することもできる。
このようなフォーマットを設けることにより、データ格納メモリに格納された全ての処理対象データのうち、たとえばＭＤ５で処理の中断を行う必要がある処理対象データに対しては、転送データ位置と転送データサイズとＭＤ５と中断の指示を、またたとえば、ＳＨＡ－１で処理の再開を行う必要がある処理対象データに対しては、転送データ位置と転送データサイズとＳＨＡ－１と再開の指示を、することができる。
また、ハッシュ処理の演算途中結果が保持することにより、処理の中断時にはその途中結果となるデータをストアし、処理の再開時にはストアしたデータをセットすることができ、これにより、処理の再開が容易に行われる。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正の内容】
【００２５】
本実施形態に係る暗号処理装置１０は、図１に示すように、ＣＰＵ１１、データ格納メモリ１２、データバス１３、ダイレクトメモリアクセスコントローラ（ＤＭＡＣ；Direct Memory Access Controller）１４、セレクタ回路１５、初期値（ＩＶ；Initial Value）レジスタ１６、共通鍵暗号ブロック１７、ハッシュブロック１８、ＩＶレジスタ１９、およびセレクタ回路２０を有する。
本実施形態においては、データバス１３に対して、ＣＰＵ１１、データ格納メモリ１２、ＤＭＡＣ１４、ＩＶレジスタ１６、およびＩＶレジスタ１９が接続されている。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】変更
【補正の内容】
【００２６】
本実施形態の暗号処理装置１０は、以下の特徴を有している。
ＤＭＡＣ１４は、ＤＭＡディスクリプタを、データ格納メモリ１２から処理すべき転送データを指示する情報のデータとして用い、各ＤＭＡディスクリプタは、各種のディスクリプタフォーマット（のデータ）を有することができ、このディスクリプタフォーマットに、ＤＥＳ（Data Encryption Standard）やＡＥＳ（Advanced Encryption Standard）といった共通鍵暗号の暗号アルゴリズムを指示するフィールド、ＥＣＢ（Electronic Code Book）モードやＣＢＣ（Cipher Block Chaining ）モードやカウンタモード（Counter Mode）といった暗号処理モードを指示するフィールド、等々を、含ませることができる。
これにより、データ格納メモリ１２に格納された全ての処理対象データのうち、たとえばDES-CBCモードで処理を行う必要がある処理対象データに対しては、転送データ位置と転送データサイズとＤＥＳとＣＢＣモードの指示を、またたとえば、AES-Counter Modeで処理を行う必要がある処理対象データに対しては、転送データ位置と転送データサイズと

ＡＥＳとCounter Modeの指示を、各ＤＭＡディスクリプタに基づいて、それぞれの処理対象データに対して指示可能としている。

そして、共通鍵暗号ブロック１７は、ＩＶレジスタ１６に接続されており、各種暗号処理モード(CBCモード、Counter Mode)での処理時に使用されるＩＶをセットする記憶手段と、次のブロック処理時に使用されることになるＩＶを自動生成して保持する記憶手段としての機能を有する。

これにより、次のブロック処理時に使用されるＩＶが自動生成されて保持されるため、処理の中断時はそのＩＶをストアし、処理の再開時はストアしたＩＶをセットすることにより処理の再開を容易としている。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正の内容】
【００２７】

また、本実施形態の暗号処理装置１０は、同様に、以下の特徴も有する。

すなわち、各ＤＭＡディスクリプタの各種のディスクリプタフォーマットとして、ＭＤ５（Message Digest #5 ）やＳＨＡ－１（Secure Hash Algorithm ）といったハッシュアルゴリズムを指定するフィールド、ハッシュ処理の中断の指示するフィールド、ハッシュ処理の再開を指示するフィールド、等々を、含ませることができる。

これにより、データ格納メモリ１２に格納された全ての処理対象データのうち、たとえばＭＤ５で処理の中断を行なう必要がある処理対象データに対しては、転送データ位置と転送データサイズとＭＤ５と中断の指示を、またたとえば、ＳＨＡ－１で処理の再開を行なう必要がある処理対象データに対しては、転送データ位置と転送データサイズとＳＨＡ－１と再開を、各ＤＭＡディスクリプタに基づいて、指示可能としている。

そして、ハッシュブロック１８は、ＩＶレジスタ１９に接続されており、ハッシュ処理の中断処理時に演算途中結果を保持する記憶手段と、ハッシュ処理の再開処理時に演算途中結果をセットできる記憶手段としての機能を有する。

これにより、ハッシュ処理の演算途中結果が保持されるため、処理の中断時はその途中結果となるＩＶをストアし、処理の再開時はストアしたＩＶをセットすることにより処理の再開を容易としている。

【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】変更
【補正の内容】
【００４７】

図３のブロック図で示したブロック構成において、ディスクリプタにてCounter Mode暗号化、もしくは、Counter Mode復号を指示した場合に、選択されるデータ経路を図７に実線で示す。

Counter Modeの場合は暗号化と復号では同じ経路となる。共通鍵暗号コアＢ８への入力にはＩＶを入力させ、暗号化データとしての出力は、共通鍵暗号コアＢ８の出力と処理対象データを順次エクスクルーシブＯＲしたデータを処理済みのデータとして出力させる。また、次のブロック処理時に使用されるＩＶは、ＩＶを＋１インクリメントしたデータを出力ＩＶレジスタＢ３に保持させるよう動作させる。

【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００５６
【補正方法】変更
【補正の内容】

【００５６】
ハッシュ演算コア(MD5,SHA1)Ｃ６への入力には、入力データバッファＣ１の出力データと、セレクタ回路Ｃ５の出力データが、それぞれ入力される。
セレクタ回路Ｃ５は、ＤＭＡディスクリプタにて再開無しが指示された場合は初期ＩＶ固定データＣ４の出力を選択し、再開有りが指示された場合は入力ＩＶレジスタＣ３の出力を選択する。
出力データバッファＣ９への入力には、ハッシュ演算コア(MD5,SHA-1)Ｃ６の出力データと初期ＩＶ固定データＣ７を加算回路Ｃ８で演算した結果とが入力される。
出力ＩＶレジスタＣ３への入力には、ハッシュ演算コア(MD5,SHA-1)Ｃ６の出力データが入力される。初期ＩＶ固定データＣ７と加算する前のデータ（ハッシュの処理単位である５１２バイト毎に順次出力されるデータ）が、計算途中結果となり、その計算途中データをＩＶとして保持する。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００６６
【補正方法】変更
【補正の内容】
【００６６】
以上説明したように、本実施形態によれば、ＤＭＡディスクリプタは、ＤＭＡＣ１４がデータ格納メモリ１２から処理すべき転送データを指示する情報となる。そして、ＤＭＡディスクリプタの各種ディスクリプタフォーマットとして、ＤＥＳやＡＥＳといった共通鍵暗号の暗号アルゴリズムを指示するフィールドと、ＥＣＢモードやＣＢＣモードやカウンタモード（Counter Mode）といった暗号処理モードを指示するフィールドとを含ませることができる。このため、データ格納メモリに格納された処理対象データに対して、対応する処理内容、たとえばDES-CBC暗号化やAES-Counter Mode暗号化などと転送データ位置および転送サイズをそれぞれ指定することが可能となる。
これにより、処理対象データのサイズと処理モードが確定した時点でＣＰＵはディスクリプタを生成してＤＭＡ処理を依頼するだけとなるため、効率的に暗号化処理を行うことができる。
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００６８
【補正方法】変更
【補正の内容】
【００６８】
また、本実施形態によれば、各ＤＭＡディスクリプタの各種のディスクリプタフォーマットとして、ＭＤ５（Message Digest #5 ）やＳＨＡ－１（Secure Hash Algorithm ）といったハッシュアルゴリズムを指定するフィールド、ハッシュ処理の中断の指示するフィールド、ハッシュ処理の再開を指示するフィールド、等々を、含ませることができる。このため、データ格納メモリに格納された処理対象データに対して、対応する処理内容たとえばＭＤ５の中断処理やＳＨＡ－１の再開処理などと転送データ位置及び転送サイズをそれぞれ指定することが可能となる。
これにより、処理対象データのサイズと処理モードが確定した時点でＣＰＵ１１はＤＭＡディスクリプタを生成してＤＭＡ処理を依頼するだけとなるため、暗号化処理と同様にハッシュ処理に関しても効率的に処理を行うことができる。