【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３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2005-505069(P2005-505069A)
【公表日】平成17年2月17日(2005.2.17)
【年通号数】公開・登録公報2005-007
【出願番号】特願2003-533509(P2003-533509)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｈ０４Ｌ　 9/10　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５４０Ａ
Ｈ０４Ｌ　 9/00　　６２１Ｚ

【手続補正書】
【提出日】平成17年9月8日(2005.9.8)
【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】
暗号化された形態でメモリにデータワードを記憶するためのシステムであって、前記データワードは各々の関連するアドレスによって特定され、前記システムは、
前記関連するアドレスの制御下でデータワードを暗号化するための暗号化器
を含み、前記暗号化器は、
ハッシュされたアドレスに前記関連するアドレスを変換するためのハッシュ関数部と、
前記ハッシュされたアドレスに前記データワードを結合させるための結合器と、
暗号化されたワードに前記結合されたワード／ハッシュされたアドレスを暗号化するためのブロック暗号部と、
前記関連するアドレスの制御下で前記メモリに前記暗号化されたワードを書き込むための書き込み器と、
前記ワードに関連するアドレスの制御下でメモリから暗号化されたワードを読み出すための読み出し器と、
前記関連するアドレスの制御下で前記読み出された暗号化されたワードを復号化するための復号化器と
を含み、前記復号化器は、
前記暗号化器によって使用されるものと同じである、ハッシュされたアドレスに前記関連するアドレスを変換するためのハッシュ関数部と、
前記暗号化器の前記ブロック暗号部の逆関数である、前記暗号化されたワードを復号化するためのブロック暗号部と、
前記ハッシュされたアドレスに前記復号化されている暗号化されたワードを結合させることによってデータワードを取り出すための分離器と
を含むシステム。
【請求項２】
前記復号化器において、前記ハッシュ関数部及び前記ブロック暗号部が並列に構成される請求項１に記載のシステム。
【請求項３】

前記暗号化器の前記ブロック暗号部及び前記ハッシュ関数部が、同じ所定のブロック暗号部のラウンドを使用する請求項１に記載のシステム。
【請求項４】
前記所定のブロック暗号部が、既定数のｎラウンドを有し、前記ハッシュ関数部が、前記所定のブロック暗号部のｋラウンドを使用し、１<＝ｋ<ｎであり、前記暗号化器の前記ブロック暗号部は、前記所定のブロック暗号部のｎ－ｋラウンドを使用する請求項３に記載のシステム。
【請求項５】
ｋ>＝３及びｎ－ｋ>＝３となる請求項４に記載のシステム。
【請求項６】
ｎ＝ｋとなる請求項４に記載のシステム。
【請求項７】
前記データワードが複数のコンポーネントを含み、前記システムは、
前記データワードに関連するアドレスの制御下でメモリから暗号化されたワードを読み出すために前記読み出し器を使用するステップと、
ハッシュされたアドレスに前記関連するアドレスを変換するために前記ハッシュ関数部を使用するステップと、
前記暗号化されたワードを復号化するために前記復号化器の前記ブロック暗号部を使用するステップと、
前記ハッシュされたアドレスの制御下で前記新たなコンポーネント値を前記復号化されている暗号化されたワードに結合させるためにコンポーネント更新器を使用し、更新されている結合されたワード／ハッシュされたアドレスを形成するステップと、
更新されている暗号化されたワードに、前記更新されている結合されたワード／ハッシュされたアドレスを暗号化するための前記暗号化器の前記ブロック暗号部を使用するステップと
によって新たなコンポーネント値に前記データワードのコンポーネントを更新するように動作する請求項１に記載のシステム。
【請求項８】
請求項１に記載される、メモリに暗号化された形態でデータワードを記憶させるためのシステムにおける使用のための暗号化器であって、前記各々のデータワードは各々関連するアドレスによって特定され、前記暗号化器は、
データワードに関連するアドレスをハッシュされたアドレスに変換するためのハッシュ関数部と、
前記ハッシュされたアドレスに前記データワードを結合させるための結合器と、
暗号化されたワードに前記結合されたワード／ハッシュされたアドレスを暗号化するためのブロック暗号部と
を含む暗号化器。
【請求項９】
請求項１に記載される、メモリに暗号化された形態でデータワードが記憶されるシステムにおける使用のための復号化器であって、前記各々のデータワードは各々関連するアドレスによって特定され、前記復号化器は、
前記メモリにおけるデータワードに関連するアドレスをハッシュされたアドレスに変換するためのハッシュ関数部と、
前記関連するアドレスの制御下で前記メモリから読み出されている暗号化されたワードを復号化するためのブロック暗号部と、
前記ハッシュされたアドレスに前記復号化されている暗号化されたワードを結合させることによって平文データワードを取り出すための分離器と
を含む復号化器。
【請求項１０】
暗号化された形態でのメモリにおける記憶のためにデータワードを暗号化する方法であ

って、前記各々のデータワードは各々関連するアドレスによって特定され、前記方法は、
データワードに関連するアドレスをハッシュされたアドレスに変換するステップと、
前記ハッシュされたアドレスに前記データワードを結合させるステップと、
前記メモリにおける後続する記憶のために、暗号化されたワードに前記結合されたワード／ハッシュされたアドレスを暗号化するためにブロック暗号部を使用するステップと
を含む方法。
【請求項１１】
暗号化された形態でメモリに記憶されるデータワードを復号化する方法であって、前記各々のデータワードは各々関連するアドレスによって特定され、前記方法は、
前記メモリにおいて記憶される暗号化されたデータワードに関連するアドレスをハッシュされたアドレスに変換するステップと、
前記関連するアドレスの制御下で前記メモリから読み出されている前記暗号化されたデータワードを中間形態に復号化するためにブロック暗号部を使用するステップと、
前記ハッシュされたアドレスに前記中間形態を結合させることによって平文データワードを取り出すステップと
を含む方法。
【請求項１２】
請求項１０に記載の方法をプロセッサに実行させるように動作するコンピュータプログラム。
【請求項１３】
請求項１１に記載の方法をプロセッサに実行させるように動作するコンピュータプログラム。