【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】平成28年6月30日(2016.6.30)

【公開番号】特開2013-247676(P2013-247676A)
【公開日】平成25年12月9日(2013.12.9)
【年通号数】公開・登録公報2013-066
【出願番号】特願2013-100918(P2013-100918)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｄ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０６Ｆ　21/24　１６６Ｃ

【手続補正書】
【提出日】平成28年5月11日(2016.5.11)
【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】
第１記憶装置に格納された第１プリミティブＩＤを提供され、前記第１プリミティブＩＤから前記第１記憶装置の固有識別子である第１メディアＩＤを演算するＩＤ演算部と、
ユーザを認証するための認証情報をセキュア鍵生成部に提供する認証情報提供部と、
前記第１メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成するセキュア鍵生成部を含むセキュア鍵生成装置。
【請求項２】
前記第１プリミティブＩＤは、前記第１メディアＩＤ演算に用いる一つ以上の識別用データであり、前記第１メディアＩＤとは異なるデータである請求項１に記載のセキュア鍵生成装置。
【請求項３】
前記第１プリミティブＩＤは、前記第１記憶装置に備えられた第１メモリ素子の固有識別子である第１メモリＩＤを暗号化した第１暗号化メモリＩＤであり、
前記ＩＤ演算部は、前記第１暗号化メモリＩＤを前記第１メモリＩＤで復号化し、前記第１メモリＩＤから第１メモリ派生ＩＤを演算し、前記第１メモリ派生ＩＤを前記第１メディアＩＤとして使用する請求項１に記載のセキュア鍵生成装置。
【請求項４】
前記第１プリミティブＩＤは、前記第１記憶装置に備えられたコントローラの固有識別子である第１コントローラＩＤを含み、
前記ＩＤ演算部は、前記第１コントローラＩＤを用いて前記第１メディアＩＤを演算する請求項１に記載のセキュア鍵生成装置。
【請求項５】
前記第１プリミティブＩＤは、前記第１記憶装置に備えられた第１メモリ素子の固有識別子である第１メモリＩＤを暗号化した第１暗号化メモリＩＤ及び前記第１記憶装置に備

えられた第１コントローラの固有識別子である第１コントローラＩＤを含み、
前記ＩＤ演算部は、前記第１暗号化メモリＩＤを前記第１メモリＩＤで復号化し、前記第１メモリＩＤから第１メモリ派生ＩＤを演算し、前記第１コントローラＩＤ及び前記第１メモリ派生ＩＤを全て用いて前記第１メディアＩＤを演算する請求項１に記載のセキュア鍵生成装置。
【請求項６】
前記認証情報提供部は、前記ユーザから前記認証情報を入力され、
前記セキュア鍵生成部は、前記第１メディアＩＤとユーザから入力された認証情報を全て用いて前記セキュア鍵を生成する請求項１に記載のセキュア鍵生成装置。
【請求項７】
記憶装置に格納されたプリミティブＩＤを提供され、プロセッサに提供する記憶装置インターフェースと、
前記プリミティブＩＤから前記記憶装置の固有識別子であるメディアＩＤを演算し、前記メディアＩＤ及びユーザを認証するための認証情報を全て用いてセキュア鍵を生成するプロセッサを含むセキュア鍵生成装置。
【請求項８】
メモリ素子の固有識別子であるメモリＩＤ及び前記メモリＩＤを暗号化した暗号化メモリＩＤを格納するメモリ素子と、
ホスト装置からユーザを認証するための認証情報を提供され、セキュア鍵生成部に提供し、前記ホスト装置からコンテンツを提供され、暗号化部に提供するホストインターフェースと、
前記メモリ素子から前記暗号化メモリＩＤを読み込み、前記暗号化メモリＩＤを復号化して前記メモリＩＤを取得し、前記メモリＩＤを用いて前記メモリ素子の他の固有識別子であるメモリ派生ＩＤを生成する派生ＩＤ演算部と、
前記認証情報及び前記前記メモリ派生ＩＤを全て用いてセキュア鍵を生成するセキュア鍵生成部と、
前記セキュア鍵を用いて前記コンテンツを暗号化して前記メモリ素子に格納する暗号化部を含む記憶装置。
【請求項９】
前記認証情報は、ＳＤカード規格（ＳＤ　Ｃａｒｄ　Ｓｔａｎｄａｒｄ）コマンドのパラメータとして含まれて前記ホスト装置から提供される請求項８に記載の記憶装置。
【請求項１０】
記憶装置をセキュア鍵生成装置に電気的に接続し、
前記セキュア鍵生成装置が前記記憶装置に格納されたプリミティブＩＤを提供され、前記プリミティブＩＤから前記記憶装置の固有識別子であるメディアＩＤを演算し、
前記セキュア鍵生成装置がユーザから前記ユーザを認証するための認証情報を直接入力されるか、またはネットワークを介して接続された他の装置から前記認証情報を提供され、
前記セキュア鍵生成装置が前記メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成することを含むセキュア鍵の生成方法。