【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I664555
【45】公告日： 中華民國 108 (2019) 年 07 月 01 日
【51】Int. Cl.：　*G06F21/84　(2013.01)*　　*G06F21/30　(2013.01)*
發明　　全 4 頁

【54】名　　稱：手持裝置的顯示屏和主機板之間的密鑰配對方法及利用其之手持裝置

【21】申請案號：106142030　　【22】申請日： 中華民國 106 (2017) 年 11 月 30 日
【11】公開編號：201926120　　【43】公開日期： 中華民國 108 (2019) 年 07 月 01 日

【72】發 明 人： 李坤 (CN) ；徐東 (CN) ；樊磊 (CN) ；張晉芳 (CN)
【71】申 請 人： 大陸商北京集創北方科技股份有限公司　CHIPONE TECHNOLOGY(BEIJING) CO.,LTD
臺北市中正區中國大陸
【74】代 理 人： 葉盛豐

【56】參考文獻：

TW	201217186A	TW	201535142A
CN	106355077A	US	2011/0093702A1
US	2013/0047272A1		

審查人員：李國隆

【57】申請專利範圍

1. 一種手持裝置的顯示屏和主機板之間的密鑰配對方法，其包含以下步驟：一主機板向一顯示屏請求獲取一 ID 序列號；該顯示屏傳送該 ID 序列號至該主機板；該主機板依該 ID 序列號產生一分散密鑰並將該分散密鑰傳送至該顯示屏，該分散密鑰的計算方式係依一手機終端廠商的品牌類型、生產批次及平臺類型設定一共用密鑰，再依該共用密鑰與該 ID 序列號的一填充後雜湊值進行一加密運算，其中，該填充後雜湊值係該 ID 序列號經一填充函式及一雜湊函式處理後而產生；該顯示屏將該分散密鑰預置為一初始密鑰；以及該顯示屏傳送一密鑰預置成功通知至該主機板。
2. 如申請專利範圍第 1 項所述之手持裝置的顯示屏和主機板之間的密鑰配對方法，其中該加密運算包含一對稱密碼演算法。
3. 如申請專利範圍第 1 項所述之手持裝置的顯示屏和主機板之間的密鑰配對方法，其中該初始密鑰係儲存於該顯示屏底下的一積體電路的一快閃記憶體(Flash)中。
4. 如申請專利範圍第 1 項所述之手持裝置的顯示屏和主機板之間的密鑰配對方法，其進一步包含以下步驟：該主機板向該顯示屏請求建立連接，並啟動一認證程序；該顯示屏傳送該 ID 序列號及一待認證狀態備妥信號至該主機板；該主機板傳送一隨機數至該顯示屏；該顯示屏利用該初始密鑰對該隨機數進行一加密程序以產生一加密結果並將該隨機數及該加密結果傳送至該主機板；該主機板對該加密結果進行一認證程序以產生一認證結果；以及該主機板依該認證結果決定是否和該顯示屏建立連接。
5. 一種手持裝置，其係利用如申請專利範圍第 1-4 項中之任一項所述之手持裝置的顯示屏和主機板之間的密鑰配對方法而防止其內含資訊被盜取。

圖式簡單說明

圖 1 為應用本發明之方法之一手持裝置方塊圖。 圖 2 為本發明之方法之一第一組流程之流程圖。 圖 3 為本發明之方法之一第二組流程之流程圖。

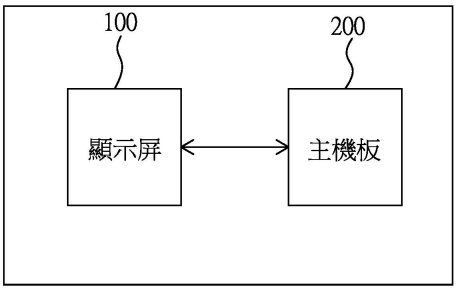

圖 1

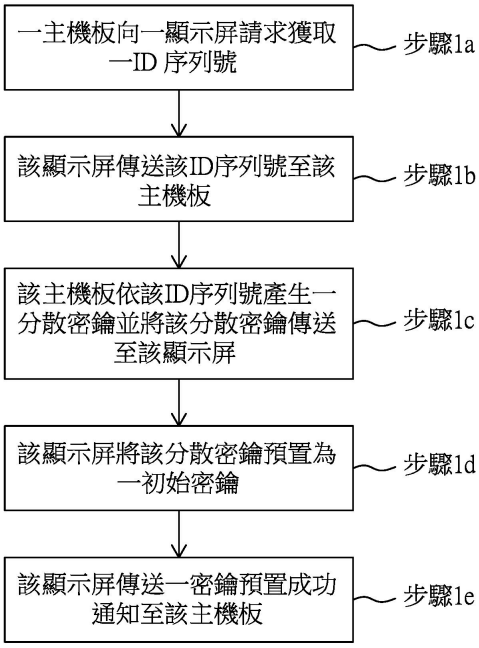
一主機板向一顯示屏請求獲取一ID 序列號
步驟1a
該顯示屏傳送該ID序列號至該主機板
步驟1b
該主機板依該ID序列號產生一分散密鑰並將該分散密鑰傳送至該顯示屏
步驟1c
該顯示屏將該分散密鑰預置為一初始密鑰
步驟1d
該顯示屏傳送一密鑰預置成功通知至該主機板
步驟1e

圖 2

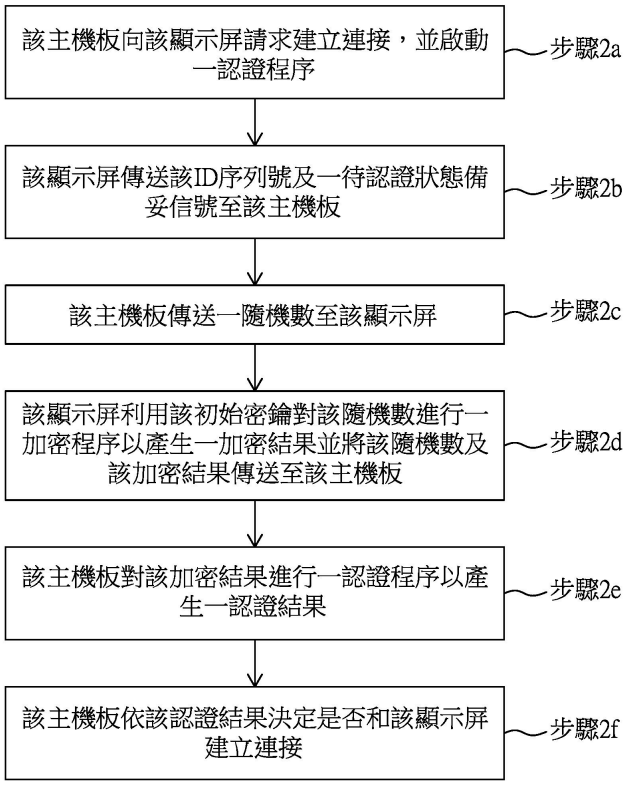
該主機板向該顯示屏請求建立連接，並啟動一認證程序
步驟2a
該顯示屏傳送該ID序列號及一待認證狀態備妥信號至該主機板
步驟2b
該主機板傳送一隨機數至該顯示屏
步驟2c
該顯示屏利用該初始密鑰對該隨機數進行一加密程序以產生一加密結果並將該隨機數及該加密結果傳送至該主機板
步驟2d
該主機板對該加密結果進行一認證程序以產生一認證結果
步驟2e
該主機板依該認證結果決定是否和該顯示屏建立連接
步驟2f

圖 3