Missing data/Data saknas

SAMMANDRAG

En elektronisk krypteringsapparat för kryptering av datafiler, innefattande en kryptomodul (113) konfigurerad att läsa en eller flera okrypterade datafiler lagrade i ett första filsystem på ett första externt minne (107); kryptera nämnda en eller flera datafiler till en eller fler krypterade datafiler; och skriva nämnda en eller flera krypterade datafiler till ett andra filsystem på ett andra externt minne (108).

Att publiceras med FIG 2.

ELEKTRONISK KRYPTERINGSAPPARAT OCH METOD

Tekniskt område

Föreliggande uppfinning hänför sig allmänt till det tekniska området elektroniska krypteringsapparater och mer specifikt till elektroniska krypteringsapparater och metoder för kryptering av datafiler.

Bakgrund

Universal Serial Bus (USB) är en specifkation för att etablera kommunikation mellan enheter och en värdkontrollenhet, såsom PCar (persondatorer).

USB kan förbinda datorpereferienheter såsom möss, tangentbord, digitalkameror, skrivare, personliga mediaspelare, flashminnen och externa hårddiskar. Trots att USB designades för persondatorer, har det blivit vanligt på andra enheter såsom smartphones, personliga digitala assistenter (PDA) och tv-spelsenheter. För många av dessa enheter har USB blivit standardmetod för anslutning.

Ett USB-minne består av en flashminnesenhet för datalagring integrerad med ett USB-gränssnitt och är typiskt portabelt och överskrivbart.

Eftersom USB-minnen är portabla kan de också enkelt förkommas eller bli stulna. USB-minnen kan därför få innehållet krypterat med hjälp av tredjepartskrypteringsmjukvara eller program som kan använda krypterade arkiv såsom ZIP och RAR. De exekverbara filerna kan lagras på USB-minnet tillsammans med den krypterade filbilden. Den krypterade partitionen kan då kommas åt på valfri dator som kör rätt operativsystem, fastän det kan krävas att användare har administrativa rättigheter på värddatorn för att komma åt data. Ett problem med detta är att krypteringsmjukvaran eller programmen måste vara installerade på en specifik PC och kräver specifika operativsystem.

Några leverantörer har producerat USB-minnen, som använder hårdvarubaserad kryptering som en del av designen, vilket sålunda tar bort kravet på tredjepartskrypteringsmjukvara. Andra flashminnen låter användaren konfigurera säkra och publika partitioner av olika storlek, och erbjuder hårdvarukryptering. Ett problem med krypterade partitioner är emellertid bristen på transparens för värddatorn.

Ett annat tillvägagångssätt att tillhandahålla krypterad information på ett portabelt minne, såsom ett USB-minne, är en genomgångs-dangle med kryptering visad i US2007/033320. Genomgångs-danglen med kryptering gör det möjligt för olika minnesenheter med USB-gränssnitt, såsom flashminneskort eller flashminnen, att enkelt

förses med eller kopplas från en krypterings/dekrypterings-funktion. En kontrollenhet med USB-gränssnitt och datakrypterings- och dekrypteringskapacitet utför krypterings/dekrypteringsfunktionen för att generera en identitetskod för flashminnet. Om ett krypterat flashminne sätts in i USB-porten på en värddator, som inte känner igen identitetskoden, kan datorn inte komma åt data på det krypterade flashminnet och därför kan data på flashminnet skyddas. Om emellertid det krypterade flashminnet sätts in i genomgångsdanglen med kryptering, kan kontrollenheten känna igen identitetskoden och utföra dekrypteringsfunktionen på data, och datorn kan därför komma åt data från det krypterade flashminnet. Även denna metod saknar transparens för värddatorn.

En annan nackdel med tidigare känd teknik är icke-existerande eller osäker nyckelhantering.

Det finns därför ett behov av förbättrad elektronisk krypteringsutrustning.

Sammanfattning

Det ska betonas att termen "innefattar" när den används i denna specifikation avser att ange förekomsten av nämnda särdrag, enheter, steg eller komponenter, men utesluter inte förekomsten eller tillägg av en eller fler andra funktioner, enheter, steg eller komponenter, eller grupper av dessa.

Det är ett ändamål med uppfinningen att övervinna åtminstone några av ovanstående nackdelar och tillhandahålla en förbättrad elektronisk krypteringsapparat.

Enligt en första aspekt av uppfinningen, uppnås detta genom en elektronisk krypteringsapparat för kryptering av datafiler. Den elektroniska krypteringsapparaten kännetecknas av en kryptomodul konfigurerad att läsa en eller fler okrypterade datafiler lagrade i ett först filsystem på ett första externt minne; kryptera nämnda en eller flera okrypterade datafiler till en eller flera krypterade datafiler; och skriva nämnda en eller flera krypterade datafiler till ett andra filsystem på ett andra externt minne.

I några utföringsformer kan apparaten vidare innefatta en första anslutning operativt ansluten till kryptomodulen via en första filsystemenhet för överföring av nämnda en eller flera okrypterade datafiler från det första externa minnet till kryptomodulen; och en andra anslutning operativt ansluten till kryptomodulen via en andra filsystemenhet för överföring av nämnda en eller flera krypterade datafiler krypterade av kryptomodulen till det andra filsystemet på det andra externa minnet.

I några utföringsformer är kryptomodulen konfigurerad att läsa nämnda en eller fler okrypterade datafiler från ett första externt USB-minne.

I några utföringsformer är kryptomodulen konfigurerad att skriva nämnda en eller fler krypterade datafiler till ett andra filsystem på ett andra externt USB-minne.

I några utförandeformer är kryptomodulen konfigurerad att läsa nämnda en eller fler okrypterade datafiler från det andra filsystemet på det andra minnet på en extern dator.

Kryptomodulen kan i några utföringsformer vara konfigurerad att läsa nämnda en eller flera okrypterade datafiler från det andra filsystemet på en hårddisk, en CD-ROM-station, ett RAM-minne (random access memory), ett ROM-minne (read only memory), ett flashminne, optisk lagringsenhet eller magnetisk lagringsenhet.

Den elektroniska krypterinsapparaten enligt krav 1 eller 2, varvid kryptomodulen (113) är konfigurerad att skriva nämnda en eller flera krypterade datafiler till det andra filsystemet på en hårddisk, en CD-ROM-station, ett RAM-minne (random access memory), ett ROM-minne (read only memory), ett flashminne, optisk lagringsenhet eller magnetisk lagringsenhet.

Den elektroniska krypteringsapparaten kan i några utföringsformer vidare innefatta ett nyckelgränssnitt operativt anslutet till kryptomodulen för att ladda krypteringsnycklar för kryptering av nämnda en eller flera okrypterade filer.

Enligt en andra aspekt av uppfinningen uppnås detta med en metod för kryptering av data. Metoden kännetecknas av stegen att:

läsa en eller fler okrypterade datafiler lagrade i ett första filsystem på ett första externt minne;

kryptera nämnda en eller flera okrypterade datafiler till en eller fler krypterade filer; och

skriva nämnda en eller flera krypterade datafiler till ett andra filsystem på ett andra externt minne.

I några utföringsformer kan den andra aspekten dessutom ha särdrag identiska med eller motsvarande vilken som helst av de olika särdragen som beskrivits ovan för den första aspekten av uppfinningen.

En fördel med några av uppfinningens utföringsformer är att krypterings-apparaten förstår filsystemen hos minnen, som lagra okrypterade såväl som krypterade datafiler, varvid krypteringsapparaten är väsentligen transparent. Därmed möjliggör den elektroniska krypteringsapparaten obegränsat skapande/raderande av filer och kataloger och läsande/skrivande av filer på olika minnen, såväl som formatering av godtyckliga minnen anslutna till den elektroniska krypteringsapparaten.

En annan fördel med en några utföringsformer av uppfinningen är att en värddator och filkrypteringsapparaten kan samverka genom filsystemskommandon, dvs öppna, läsa, skriva och stänga.

Kort beskrivning av ritningarna

Fler ändamål, särdrag och fördelar med uppfinningen framgår av följande detaljerade beskrivning av utföringsformer av uppfinningen med hänvisning till debifogade ritningarna, på vilka:

FIG 1A illustrerar en elektronisk filkrypteringsapparat för kryptering och dekryptering av datafiler enligt några utföringsformer av uppfinningen;

FIG 1B illustrerar ett generellt blockdiagram av en elektronisk krypterings-apparat in en driftmiljö enligt några utföringsformer av uppfinningen;

FIG 2 illustrerar ett blockdiagram av den elektronisk filkrypteringsapparaten i FIG 1 enligt några utföringsformer av uppfinningen;

FIG 3A illustrerar en schematisk ritning framifrån av en utföringsform av den elektroniska krypteringsapparaten;

FIG 3B illustrerar en schematisk ritning över baksidan av en utföringsform av den elektroniska krypteringsapparaten;

FIG 4 är ett flödesschema som illustrerar steg i en metod för kryptering/ dekryptering av datafiler med den elektroniska krypteringsapparaten;

FIG 5 illustrerar ett blockdiagram av en elektronisk filkopieringskrypterings-apparat enligt några utföringsformer av uppfinningen;

FIG 6A illustrerar en elektronisk filkrypteringsapparat för kryptering och dekryptering av datafiler enligt några utföringsformer av uppfinningen;

FIG 6B illustrarar ett generellt blockdiagram av en elektronisk filkrypterings-apparat i en driftmiljö enligt några utföringsformer av uppfinningen;

FIG 7 illustrarar ett blockdiagram av en elektronisk filserverkrypteringsapparat enligt några utföringsformer av uppfinningen;

FIG 8A visar en hårdvaruarkitektur av filserverkrypteringsapparaten enligt några utförandeformer av uppfinningen;

FIG 8B visar ett FPGA-blockdiagram av filserverkrypteringsapparaten enligt några utföringsformer av uppfinningen;

FIG 9 visar ett blockdiagram av den elektroniska filkrypteringsapparaten enligt några utföringsformer av uppfinningen; och

FIG 10 visar ett blockdiagram av en elektronisk filserverkrypteringsapparat enligt några utföringsformer av uppfinningen.

Detaljerad beskrivning

Utföringsformer av uppfinningen kommer att beskrivas med hänvisning till figurerna 1-10, vilka alla schematiskt illustrerar ett exempelarrangemang enligt några utföringsformer av uppfinningen. Samma hänvisningsbeteckningar används för motsvarande särdrag i olika figurer.

FIG 1A illustrera en elektronisk filkrypteringsapparat 100 för kryptering och dekryptering av datafiler enligt en utföringsform av föreliggande uppfinning i en driftmiljö. Ett generellt blockdiagram av den elektroniska filkrypteringsapparaten 100 visas i FIG 1B, vilken kan innefatta ett chassi 101, ett kretskort 102, en första anslutning 103, en andra anslutning 104, ett användargränssnitt 105 och ett nyckelgränssnitt 106.

Kretskortet 102 är anordnat inne i chassit 101 för uppbärande av den första anslutningen 103 för inmatning och utmatning av okrypterad information och den andra anslutningen 104 för inmatning och utmatning av krypterad information.

Den första och andra anslutningen 103 och 104 kan vara USB-kontakter för att ansluta olika minnesenheter, innefattande men inte begränsat till USB-minnesenheter som till exempel USB-flashminnesenheter.

Enligt FIG 1A kan ett första USB-minne 107 med en USB-kontakt lagra okrypterade filer för kryptering med den elektroniska krypteringsapparaten 100, när det är anslutet till den första anslutningen 103 hos den elektroniska krypteringsapparaten. Ett andra USB-minne 108 med en USB-kontakt kan anslutas till den andra anslutningen 104 för att ta emot och lagra filer som krypterats av den elektroniska krypterings-apparaten 100.

Nyckelgränssnittet 106 kan utgöras av, men är inte begränsat till, ett smartcard-gränssnitt för att ladda krypteringsnycklar för användning vid kryptering/dekryptering av filer, som passerar den elektroniska krypteringsapparaten 100.

USB-minnena 107 och 108 kan vara flashminnen, vart och ett innefattande ett litet kretskort med kretselementen och en USB-kontakt, elektriskt isolerad och skyddad inuti ett hölje av plast, metall eller gummerat material. USB-kontakten kan skyddas av en avtagbar hylsa eller genom att vara indragen i minnesanordningen, trots att det inte är sannolikt att det skadas om det är oskyddat. Flashminnena kan ha en USB-kontakt av

standard typ A, som möjliggör anslutning med en port hos den elektroniska krypteringsapparaten eller på en persondator (PC).

Den elektroniska filkrypteringsapparaten 100 är försedd med en "RÖD-/SVART-separation", det vill säga den bevarar avståndet eller installations-avskärmningen mellan kretsar och utrustning, som används för att hantera hemlig klartext- eller känslig information (RÖDA signaler) och normala oskyddade kretsar och utrustning (SVART), de senare innefattande de som bär krypterade eller chiffrerade textsignaler (SVARTA signaler).

RÖD-/SVARTA-separationen uppnås med hjälp av två separata uppsättningar av varje modul förutom kryptomodulen i den elektroniska krypteringsapparaten. Ett exempel på en utföringsform av den elektroniska filkrypteringsapparaten visas i FIG 2.

Kretskortet 102 är försett med en första USB-enhet (driver) 109 förbunden med den första anslutningen 103 för att hantera kommunikationen mellan den elektroniska krypteringsapparaten 100 och det första USB-minnet 107 på den "RÖDA sidan" när den sätts in i USB-kontakten 103. En första filsystemenhet (driver) 110 anordnad på kretskortet och operativt förbunden med den första USB-enheten 109 är anpassad att hantera information på filsystemsnivå, eftersom det bara är innehållet i datafilerna som krypteras.

På den "SVARTA sidan" har kretskortet 102 en andra USB-enhet (driver) 111 anordnad och förbunden med den andra anslutningen 104 för att hantera kommunikationen mellan den elektroniska filkrypteringsapparaten 100 och det andra USB-minnet 108 för att lagra krypterade filer, när det sätts in i den andra USB-kontakten 104. En andra filsystemsenhet (driver) 112 är operativt förbunden med den andra USB-enheten 111, som också är anpassad att hantera information på filsystemsnivå.

En kryptomodul 113 ingår, som har kapacitet för kryptering och dekryptering av datafiler och tillhandahåller autentiseringskontroll av datafiler, som passerar genom den elektroniska filkrypteringsapparaten 100.

Kryptomodulen 113 är anordnad på kretskortet 102 och operativt förbunden med den första anslutningen 103 och den andra anslutningen 104. Kryptomodulen 113 är en kontrollenhet konfigurerad att ta emot datafiler i klartext från den första anslutningen 103 och genomföra kryptering av datafilerna i klartext till datafiler i kryptotext för överföring som utdata på den andra anslutningen 104.

På motsvarande sätt är kryptomodulen 113 också konfigurerad att ta emot datafiler i kryptotext från den andra anslutningen 104 och utföra dekryptering av

datafilerna i kryptotext till datafiler i klartext för överföring som utdata på den första anslutningen 103.

Varje datafil i klartext, som är lagrad på det första USB-minnet 107, kan läsas och krypteras separat i kryptomodulen 113 när USB-minnet sätts in i den första USB-kontakten 103. Datafiler av godtycklig storlek kan läsas genom streaming och kan krypteras och skickas ut på den andra anslutningen 104 och lagras som kryptotext på det andra USB-minnet 108 när detta sätts in i den andra USB-kontakten 104.

Kryptomodulen 113 exekverar funktionen för kryptering/dekryptering enligt, men är inte begränsad till, AES-GCM, som är en autentiserad krypteringsalgoritm designad för att hantera både autentisering och sekretess.

FIG 3A visar en schematisk ritning framifrån av en utföringsform av den elektoniska krypteringsapparaten 102. Användargränssnittet 105 kan innefatta, men är inte begränsat till, en display 105a och ett tangentbord 105b för att styra funktionen för kryptering/dekryptering och andra funktioner hos apparaten. Enligt en alternativ utföringsform kan användargränssnittet 105 innefatta en tryckkänslig skärm för att styra enhetens funktioner.

FIG 3B visar en schematisk ritning från baksidan av en utföringsform av den elektroniska krypteringsapparaten 102. Utöver den första och andra anslutningskontakten 103 och 104, kan den elektroniska krypteringsapparaten ha en tredje anslutningskontakt 114 för anslutning till en värddator. Den tredje anslutningskontakten kan utgöras av, men är inte begränsad till, en USB-kontakt. Dessutom kan den elektroniska krypteringsapparaten innefatta en strömkontakt 115 för strömförsörjning. Den elektroniska krypteringsapparaten kan alternativt strömförsörjas genom en värddator ansluten till den första kontakten 103 eller den tredje kontakten 114, om den finns tillgänglig.

FIG 4 är ett flödesschema, som visar stegen i en metod för kryptering/dekryptering av datafiler, som matas in i eller ut ur de två kontakterna 103 och 104 i den elektroniska krypteringsapparaten 102. I ett första steg 200 slås den elektroniska krypteringsapparaten 102 på. Den elektroniska krypteringsapparaten genomgår en bootprocess och enhetens operativsystem övertar kontrollen i steg 201. Den elektroniska krypteringsapparaten 102 har övergått i driftläge för att vara beredd att reagera på kommandon från användargränssnittet 105 och för att kommunicera med ett godtyckligt USB-minne som ansluts till någon av USB-kontakterna 103 eller 104.

USB-minnet 107 ansluts till USB-kontakten 103 i steg 202 och USB-minnet 108 ansluts till USB-kontakten 104 i den elektroniska krypteringsapparaten i steg 203.

En användare kan ansluta USB-minnena till dess respektive USB-kontakt antingen samtidigt eller en i taget i valfri ordning. Som svar på att USB-minnet 103 ansluts, etablerar kryptomodulen 113 en förbindelse genom att signalera med det första USB-minnet 103 i steg 204, skaffar åtkomst till information om filer lagrade på ett ordinärt filsystem på USB-minnet och visar informationen om filerna och/eller filkatalogerena i en filmeny på displayen 105a. Som svar på att USB-minnet 104 ansluts etablerar kryptomodulen 113 en förbindelse genom att signalera med USB-minnet 104 i steg 205 och om det redan finns några filer och/eller filkataloger lagrade i ett ordinärt filsystem på USB-minnet 104, skaffar åtkomst till information om filerna och/eller katalogerna och i det fallet visar informationen om filerna och/eller filkatalogerna i en filmeny på displayen 105a.

En utvald nyckel för kryptering/dekryptering eller en uppsättning nycklar laddas in i den elektroniska krypteringsapparaten 102 som svar på att en användare sätter in ett smartcard 116 i smartcardgränssnittet 106 i steg 206 tillsammans med en autentisering av användaren, till exempel, men inte begränsat till, att mata in en PIN (Personal Identifikation Number)-kod som gäller för det specifika smartcardet. Kryptomodulen 113 läser krypteringsnyckeln från användarens smartcard och autentiserar användaren med hjälp av PIN-koden i steg 208.

En användare kan genom användargränssnittet 105 välja en eller flera klartext- eller okrypterade filer och/eller filkataloger lagrade på det första USB-minnet 103 i steg 209 och kopiera klartextfilerna till det andra USB-minnet 104, till exempel, men inte begränsat till, drag-och-släpp på skärmen 105a i steg 210. Som svar genereras signaler som svar på kopieringen av den utvalda filen eller filerna och/eller filkatalogerna från det första USB-minnet 103 till det andra USB-minnet 104, aktiverar kryptomodulen 114 krypteringsfunktionen genom att generera åtkomstsignaler för att lästa den utvalda filen eller filerna och/eller filkatalogerna från det första USB-minnet 103 i steg 211. Den eller de utvalda klartextfilerna och/eller filkatalogerna krypteras till kryptotext eller krypterade filer av kryptomodulen 113 i steg 212 medelst krypteringsalgoritmen, som använder den laddade krypteringsnyckeln(-arna). Krypteringsmodulen lagrar den eller de krypterade filerna i ett ordinarie filsystem på det andra USB-minnet 104.

FIG 5 illustrar ett blockdiagram av en annan utföringsform av en fil-krypteringsapparat 100' för filkopiering av okrypterade datafiler, varvid de okrypterade filerna läses, krypteras och lagras som krypterade datafiler av filkrypteringsapparaten 100' till ett andra filsystem på det andra minnet 108. Kretskortet 102 är anordnad med den första USB-enheten 109 ansluten med den första anslutningen 103 för att hantera

kommunikationen mellan den elektroniska krypteringsanordningen 100 och det första USB-minnet 107 på den "RÖDA sidan" när den ansluts till USB-kontakten 103. Den första FS-(filsystems)enheten 110 anordnad på kretskortet och operativt ansluten till den första USB-enheten 109 är anpassad att hantera information på filsystemsnivå, då det endast är innehållet i datafilerna som är krypterat.

På den "SVARTA sidan" har kretskortet 102 den andra USB-enheten 111 anordnad och ansluten till den andra kontakten 104 för att hantera kommunikationen mellan den elektroniska krypteringsanordningen 100' och det andra USB-minnet 108 för lagring av krypterade filer när den ansluts till den andra USB-kontakten 104. Den andra FS-(filsystem)enheten 112 är operativt ansluten till den andra USB-enheten 111, vilken också är anpassas för att hantera information på filsystemsnivå. Kryptomodulen innefattar två block, ett filkopieringsapplikationsblock 120 och ett filsystemkrypterings-block (CRYPTFS) 122. Filkopieringsapplikationsblocket 120 är anslutet mellan den första filsystemsenheten 110 och filsystemkrypteringsblocket 122 och är konfigurerat att läsa nämnda en eller flera okrypterade datafiler från det första externa USB-minnet 107.

Filsystemkrypteringsblocket 122 har kapacitet att kryptera och dekryptera och tillhandahåller autentiseringskontroll av datafiler, som passerar den elektroniska filkrypteringsanordningen 100'. Filsystemkrypteringsblocket 122 är anslutet till fil-kopieringsapplikationsblocket 120 och den andra filsystemsenheten 112.

Både filkopieringsapplikationsblocket 120 och filsystemkrypteingsblocket är anordnade på kretskortet 102. Filsystemkrypteringsblocket 122 är en kontrollenhet konfigurerad att ta emot datafiler i klartext från den första anslutningen 103 via filkopieringsapplikationsblocket 120 och exekvera kryptering av datafilerna i klartext till datafiler med kryptotext för överföring som utdata på den andra anslutningen 104.

På motsvarande sätt är filsystemkrypteringsblocket 122 också konfigurerat att ta emot datafiler med kryptotext från den andra anslutningen 104 och exekvera dekryptering av de datafilerna med kryptotext till datafiler med klartext för överföring via filkopieringsapplikationen 120 som utdata från den första anslutningen 103.

Varje datafil med klartext, som är lagrad på det första USB-minnet 107, kan kopieras av filkopieringsapplikationsblocket 120 och krypteras separat av fil-systemkrypteringsblocket 122 när USB-minnet ansluts till den första USB-kontakten 103. Datafiler av godtycklig storlek kan läsas genom streaming och kan krypteras och matas ut på den andra kontakten 104 och lagras som kryptotextfiler på det andra USB-minnet 108 när det ansluts till den andra USB-kontakten 104.

Filsystemkrypteringsblocket 122 exekverar krypterings/dekrypteringsfunktionen enligt, men inte begränsat till, AES-GCM, vilken är en autentiserad krypteingsalgoritm designad att hantera både autentisering och sekretess.

Figurerna 6A och 6B visar en elektronisk filhanteringskrypteringsapparat 100'' för kryptering och dekryptering av datafiler enligt en utföringsform av föreliggande uppfinning i en driftmiljö. Den första och andra kontakten 103 och 104 kan vara USB-kontakter för att ansluta olika minnesenheter, innefattande, men inte begränsat till, en dator 124 för generell användning och USB-minnet 108. Den elektroniska filhanteringskrypteringsapparaten 100'' är i denna utföringsform konfigurerad att kryptera en eller flera datafiler lagrade i ett filsystem på det interna eller externa minnet hos datorn, till en eller flera krypterade datafiler; och skriva den eller de krypterade datafilerna till det externa USB-minnet 108.

Figur 7 visar ett blockdiagram av den elektroniska filhanteringskrypteringsapparaten 100'' enligt några utföringsformer av uppfinningen. En elektronisk filhanteringskrypteringsapparat 100''kan implementeras med, men är inte begränsad till, en Linux-baserad dator. Datorn 124 har en Windows-stack 125 i den här utföringsformen, innefattande en applikation 126 och en SMB/CIFS- implementering av filsystemet 127, TCP/IP 128, RNDIS-enhet 129 och en USB-värd 130.

Filhanteringskrypteringsapparaten 100'' innefattar, men är inte begränsad till, en USB-periferienhet 109' för anslutning och överföring av okrypterade datafiler till/från datorn 124 med en Windows-stack 125, en RNDISenhet 131, TCP/IP 132 operativt ansluten till SMB/CFIS-filsystemsmodulen 133 för implementering av filsystemet. En USB-värd 111' är inkluderad för anslutning och överföring av krypterade datafiler till/från USB-minnet 108 via filsystemsenheten 112'. Krypteringsmodulen 122' krypterar/dekrypterar de okrypterade/krypterade datafilerna på filsystemnivå mellan datorn 124 och USB-minnet 108.

Sålunda implementerar SMB/CIFS-modulen 133 och krypteringsmodulen 122' ett virtuellt krypterat filsystem på toppen av det fysiska filsystemet och kan därigenom kryptera datafiler transparent med hjälp av krypteringsnyckeln, som laddas via nyckelgränssnittet 106.

Den elektroniska filkrypteringsanordningen 100'' manövreras medelst MMI 105, vilket är implementerat som en applikation som startar när anordningen bootas.

Figur 8A visar en hårdvaruarkitektur för filkrypteringsanordningen enligt några utföringsformer av uppfinningen.

Designen kan vara baserad på, men är inte begränsad till, en ACME FOX G20 Linux Embedded Single Board Computer, i denna utföringsform. Ett dotterkort, (FED Board) är anslutet till datorn. Foxg20-systemet kan vara baserat på en ATMEL AT91SAM9G20 mikrokontrollenhet, som kan ha en ARM926-processor (MCU) med MMU, instruktion och data-cachar, två USB-värdportar, en USB-port, en SPI kontrollenhet, UART:er, en realtidsklocka, fast Ethernet MAC och funktionalitet som stödjer DRAM, strömförsörjningsenhet, Micro SD FLASH-kortplats.

Dotterkortet (FEB-kort) kan ha en FPGA-modul med klockgenerator, olika knappar, en smartcardgränssnittskrets, en JTAG, debugganslutning och en displaymodul.

Fox-kortet kan hantera större delen av funktionaliteten. Kommunikationen med dotterkortet kan hanteras av SPI-kommunikation för smartcardstyrenheten. RS232 kan användas för gränssnitten för display och knappar. Displayen kan vara, men är inte begränsad till, OLED. Mjukvaran till den smarta displayen kan anpassas och/eller uppgraderas.

FPGAn kan vara, men är inte begränsad till, en Lattice XP2-enhet. Designen kan vara uppdela i, men är inte begränsad till, två huvuddatavägar. SPI-till-smartcard-vägen och MMI-vägen, som visas i figur 8B. Det är en kontextuell skillnad mellan kryptografiska nycklar och fysiska nycklar (knappar) som kan tryckas in av användaren.

SPI-till-smartcard-vägen kan tillåta värd-MUC:en att komma åt ett smartcard via sitt SPI-gränssnitt. Det kan innefatta en SPI-slav, styrlogik med register och ett smartcardkontrollblock.

SPI-slaven kan väsentligen vara, men är inte begränsad till, två 8-skiftsregister, vilka kan klockas av SPCK. SPI-klockan kan vara asynkron med huvudklockan. Alltså kan klar-pulsen(ready strobe) från slaven fångas in (synkroniseras) och förses med ny tidsinformation innan data lagras i SC-kontrollblocket.

I SC-styrkommandon, kan status och nyckeldata skiftas in/ut, men är inte begränsat till, 8 bitar i taget.

Det största blocket kan vara smartcard-kontrollenheten. Den kan hantera både smartcardprotokollet och de NBK-kortspecifika detaljerna.

MMI-vägen kan ha ett antal knappar. Knappinmatningar aktiveras (debounced) och information om knapptryckningshändelser och vilka knappar som trycks ned kan skickas till värden seriellt med UART. LED:er kan slås på valfritt genom att signallera i motsatt riktning.

Den seriella anslutningen från värden till displayen kan vidarekopplas elektriskt genom FPGA:n.

Den externa klockinsignalen (33MHz i denna utföringsform) är vidarekopplad to en PLL, vilken är konfigurerad att dividera med 3 med avsikt att generera en huvudklocka på 11 MHz i denna utföringsform. Andra externa klockfrekvenser och huvudklockfrekvenser kan användas i andra utföringsformer. SPI-slavblocket kan inte drivas av klockan.

En återställning kan genereras som eller-inte-funktion i den externa återställningsinsignalen och PLL-låssignalen.

FIG 9 illustrerar ett blockdiagram med den elektroniska filkrypteringsapparaten enligt några utföringsformer av uppfinningen, varvid krypteringsmodulen 113'' är en separat hårdvarumodul.

FIG 10 illustrerar ett blockdiagram med en elektronisk filhanterings-krypteringsapparat enligt några utföringsformer av uppfinningen, varvid krypterings-modulen 122'' är en separat hårdvarumodul.

Den elektroniska krypteringsapparaten 100 kan innefatta en digital elektronisk dator eller datorutrustning och processer utförda i en dator eller datorsystem. Datorn kan innefatta ett databehandlingssystem, innefattande en dataprocessor med kryptomodulen 113 för att behandla data, och lagringsorgan anslutna till datorprocessorn för att lagra data på ett lagringsmedium.

Den elektroniska krypteringsapparaten kan realiseras som en elektronisk apparat med manipuleringsskydd (tamper protection), dvs innefatta skydd mot åtkomst till de elektroniska kretsarna i krypteringsapparaten, information som finns i de elektroniska kretsarna (som programkod eller kretskonfiguration) eller interna signaler genererade av de elektroniska kretsarna. Dessutom eller alternativt kan manipuleringsskydd hos den elektroniska krypteringsapparaten omfatta att försök till åtkomst av de elektroniska kretsarna, information eller signaler detekteras.

Uppfinningen har beskrivits med hänvisning till olika utföringsformer. En fackman kan emellertid identifiera många variationer till de beskrivna utföringsformerna, som fortfarande ligger inom skyddsomfånget för uppfinningen. Det bör exempelvis observeras att i beskrivningen av utföringsformer av uppfinningen, indelningen av de funktionella blocken i specifika enheter inte på något sätt begränsar uppfinningen. Tvärtom är dessa indelningar bara exempel. Funktionella block, som är beskrivna som en enhet, kan delas upp i två eller flera enheter. På samma sätt kan

funktionella block, som beskrivits som implementerade i två eller flera enheter, implementeras som en enhet utan att avvika från uppfinningens skyddsomfång.

Sålunda ska det uppfattas så att avgränsningarna i de föreslagna utföringsformerna endast är för illustration och inte på något sätt är begränsande. Uppfinningens omgång framgår av patentkraven snarare än av beskrivningen och alla variationer som faller inom patentkravens omfång ska omfattas.

Föreliggande uppfinning kan realiseras som en metod i en apparat, som en apparat eller som ett system med en datorprogramprodukt. Följaktligen kan föreliggande uppfinning vara i form av en komplett hårdvaruutföringsform, eller en utföringsform som kombinerar mjukvaru- och hårdvaruaspekter, som häri allmänt refereras som en enhet, komponent eller apparat. Vidare kan mjukvaran enligt uppfinningen vara i form av en datorprogramprodukt. Datorprogramprodukten kan lagras på ett lagringsmedium för datorbruk med programkod lagrad på mediet. Utföringsformerna av uppfinningen beskrivna med hänvisningar till ritningarna innefattar en dator och processer, som utförs på datorn. Programmet kan vara i form av källkod, objektkod, kod lämplig för användning i en implementation av metoden enligt uppfinningen. Bäraren kan vara en godtycklig enhet, som har möjlighet att transportera programmet. Till exempel kan bäraren vara ett inspelningsbart medium, datorminne, skrivskyddat minne eller en elektrisk bärarsignal. Utföringsformer enligt uppfinningen kan utföras när datorprogramprodukten är laddad och körs på ett system som har datorkapacitet.

Även om uppfinningen har beskrivits med hänvisning till utföringsformer konfigurerade för USB-minnen, kan andra utföringsformer av den elektroniska krypteringsapparaten konfigureras att fungera på godtyckligt lämpligt datormedium inklusive hårddiskar, CD-ROM, RAM-minne, ROM-minnen, flashminnen, optiska lagringsenheter eller magnetiska lagringsenheter externt anslutna till den elektroniska krypteringsapparaten direkt eller indirekt via till exempel en dator.

Utföringsformer av föreliggande uppfinning har beskrivits ovan med hänvisning till flödesscheman och/eller blockdiagram. Det ska förstås att några eller alla av de illustrerade blocken kan implementeras med hjälp av datorprograminstruktioner. Dessa datorprogramsinstruktioner kan matas in till en processor i en dator för generellt bruk, en dator för specifikt bruk eller andra programmerbara databehandlingsapparater för att producera en maskin, så att instruktionerna när de exekveras skapar medel för att implementera funktionerna/handlingarna, som är angivna i flödesschemat enligt ovan.

Det ska förstås att funktionerna/handlingarna beskrivna i flödesschemat kan utföras i annan ordning än som beskrivs i funktionsbeskrivningen. Till exempel kan två block, som visas utföras efter varandra, utföras samtidigt eller ibland i omvänd ordning, beroende på funktionerna/handlingarna i det aktuella fallet. Även om en del av diagrammen innehåller pilar för kommunikationsvägar för att visa den primära kommunikationsriktningen, ska det förstås att kommunikationen kan genomföras i motsatt riktning till pilarna.

En datorprogramprodukt kan innefatta datorprogramkodavsnitt för att exekvera metoden, som beskrivits i beskrivningen och patentkraven, för att tillhandahålla styrdata när datorprogramkodavsnitten körs av en elektronisk apparat med datorkapacitet.

Ett datorlagringsmedium med en lagrad datorprogramprodukt kan innefatta datorprogramkodavsnitt för att exekvera metoden, som beskrivits i beskrivningen och patentkraven, för att tillhandahålla styrdata när datorprogramkodavsnitten körs av en elektronisk apparat med datorkapacitet.

De många särdragen och fördelarna hos uppfinningen är uppenbara från den detaljerade beskrivningen, och det är ändamålet med de bifogade patentkraven att täcka alla sådana funktioner och fördelar hos uppfinningen, som faller inom uppfinningstanken. Trots att utföringsformer av metoden och apparaten enligt uppfinningen har illustrerats i de bifogade ritningarna och beskrivits i den detaljerade beskrivningen ovan, är beskrivningen endast illustrativ, och ändringar, modifieringar och utbyten kan utföras utan att avvika från uppfinningens omfång så som den beskrivs i de följande kraven.

Terminologi:

CIFS	Common Internet File System
GPIO	General Purpose Input/Output
JTAG	Joint Test Action Group
MAC	Medium Access Controller
MCU	Micro Controller Unit
MMI	Man Machine Interface
NBK	Key Card
OLED	Organic Light Emitting Diod
RNDIS	Remote Network Driver Interface Specification
SD	Secure Digital
SMB	Server Message Block
SPI	Serial Peripheral Interface
UART	Universal Asynchronous Receiver Transmitter

VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuit

PATENTKRAV

1. Elektronisk krypteringsapparat för kryptering av datafiler, **kännetecknad** av en kryptomodul (113) konfigurerad att läsa en eller fler okrypterade datafiler lagrade i ett första filsystem på ett första externt minne (107); kryptera nämnda en eller flera datafiler till en eller fler krypterade datafiler och skriva nämnda en eller flera krypterade datafiler till ett andra filsystem på ett andra externt minne (108).

2. Elektronisk krypteringsapparat enligt krav 1, innefattande:

en första anslutning (103) operativt förbunden med kryptomodulen (113) via en första filsystemenhet (110) för överföring av nämnda en eller flera okrypterade datafiler, lästa från det första externa minnet (107), till kryptomodulen (113); och

en andra anslutning (104) operativt förbunden med kryptomodulen (113) via en andra filsystemenhet (112) för överföring av nämnda en eller flera krypterade filer krypterade av kryptomodulen (113) till det andra filsystemet på det andra externa minnet (108).

3. Elektronisk krypteringsapparat enligt krav 1 eller 2, varvid kryptomodulen (113) är konfigurerad att läsa nämnda en eller flera okrypterade datafiler från en första extern USB-minnesenhet (107).

4. Elektronisk krypteringsapparat enligt krav 1 till 3, varvid kryptomodulen (113) är konfigurerad att skriva nämnda en eller flera datafiler till det andra filsystemet på en andra extern USB-minnesenhet (108).

5. Elektronisk krypteringsapparat enligt krav 1eller 2, varvid kryptomodulen (113) är konfigurerad att läsa nämnda en eller flera okrypterade datafiler från det andra filsystemet på det andra externa minnet på en extern dator (124).

6. Elektronisk krypteringsapparat enligt krav 1 eller 2, varvid kryptomodulen (113) är konfigurerad att läsa nämnda en eller flera okrypterade datafiler från det andra filsystemet på en hårddisk, en CD-ROM-station, ett RAM (Random Access Memory), ett ROM (Read Only Memory), ett flashminne, en anordning för optisk lagring eller en anordning för magnetisk lagring.

7. Elektronisk krypteringsapparat enligt krav 1 eller 2, varvid krypto-modulen (113) är konfigurerad att skriva nämnda en eller flera krypterade datafiler till det andra filsystemet på den andra externa minnesanordningen på en hårddisk, en CD-ROM-station, ett RAM (Random Access Memory), ett ROM (Read Only Memory), ett flashminne, en anordning för optisk lagring eller en anordning för magnetisk lagring.

8. Elektronisk krypteringsapparat enligt krav 1 till 7, vidare innefattande ett nyckelgränssnitt (106) operativt förbundet med kryptomodulen (113) för att ladda krypteringsnycklar för kryptering av nämnda en eller flera okrypterade filer.

9. Metod för kryptering av data, kännetecknad av stegen att:

läsa en eller fler okrypterade datafiler lagrad i ett första filsystem på ett första externt minne (107);

kryptera nämnda en eller flera okrypterade filer till en eller fler krypterade datafiler; och

skriva nämnda en eller flera krypterade filer till ett andra filsystem på ett andra externt minne (108).

4646190525

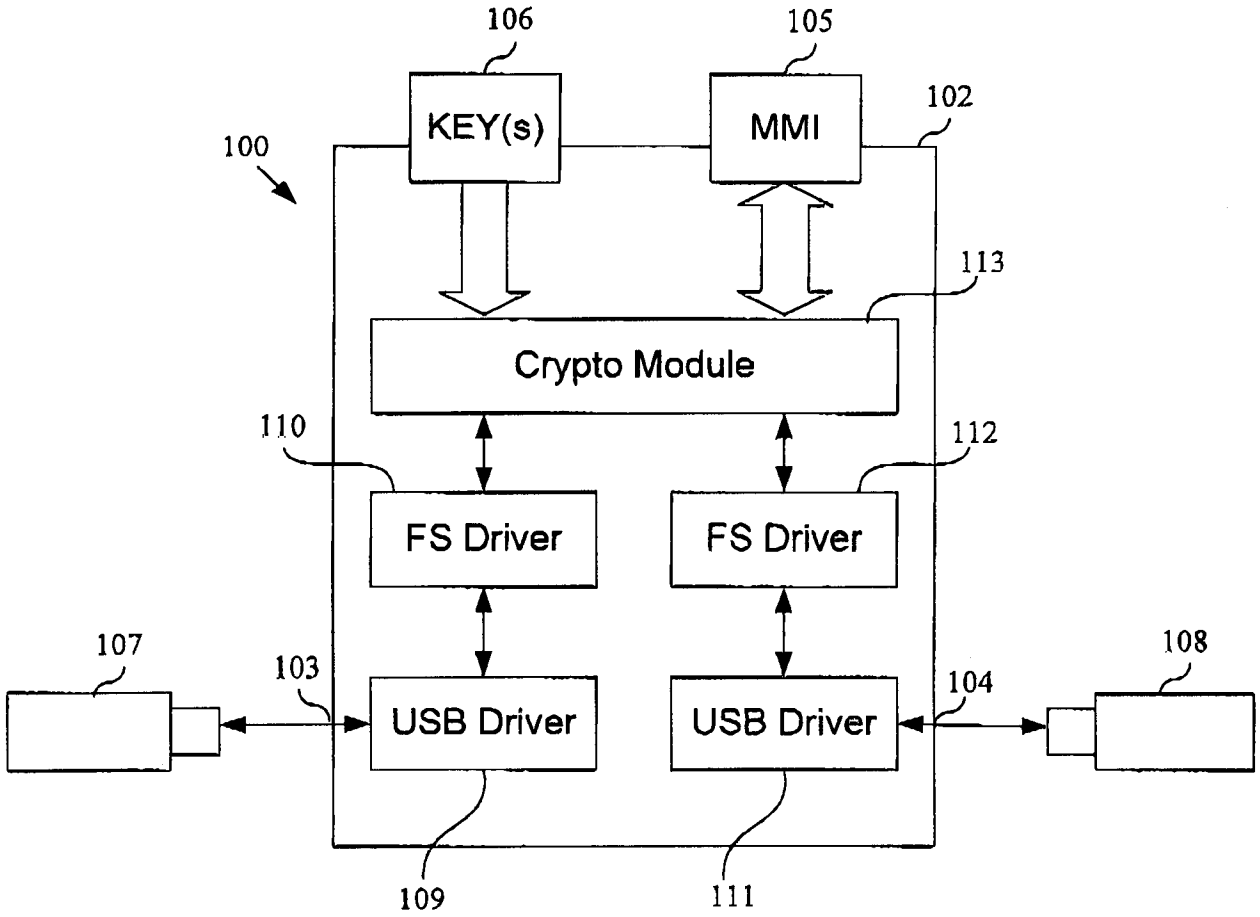

Fig. 2

4646190525

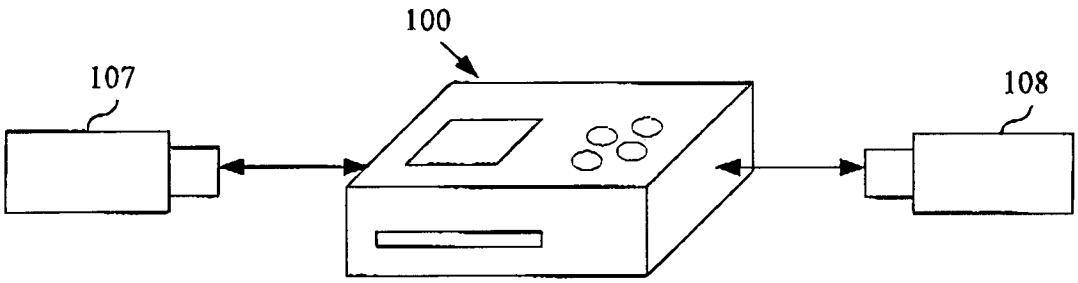

Fig. 1A

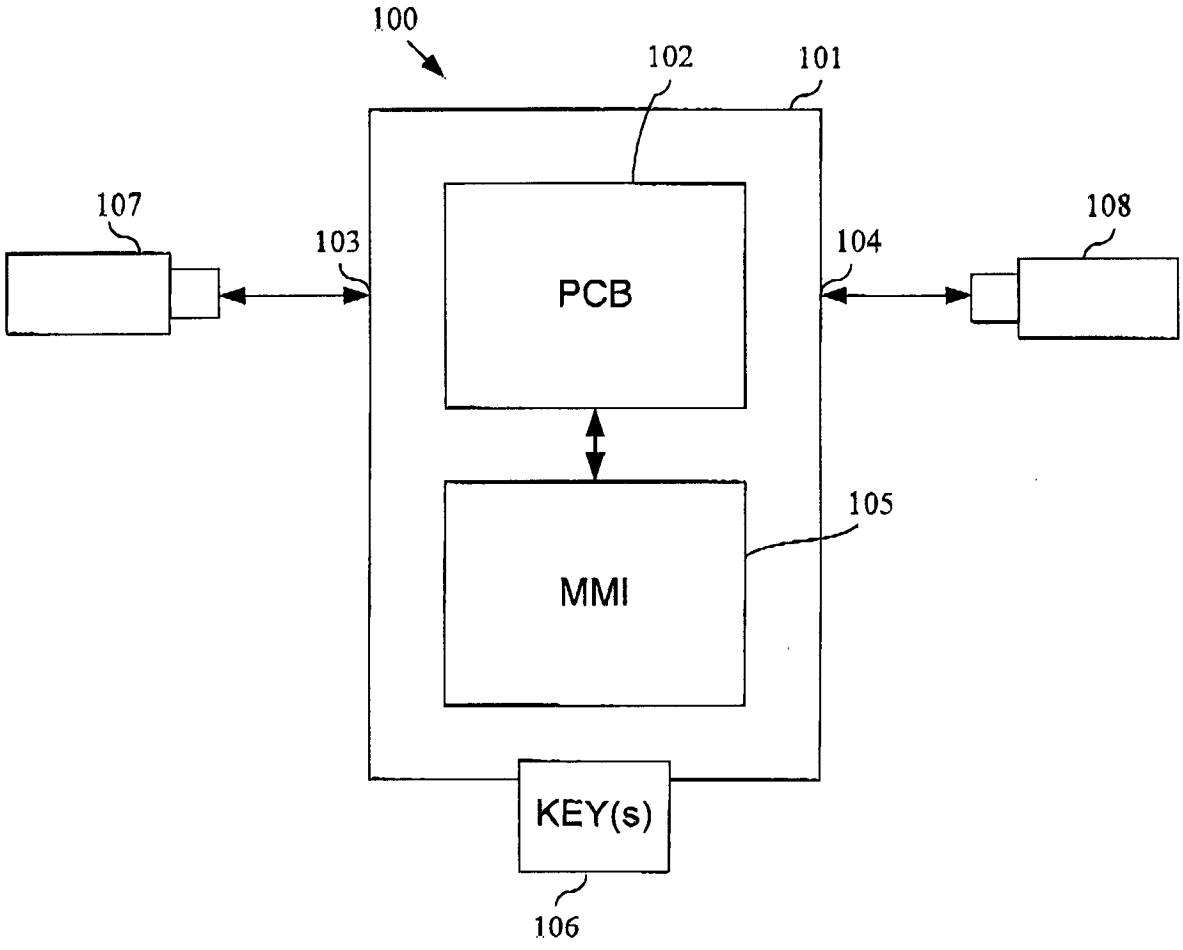

Fig. 1B

4646190525

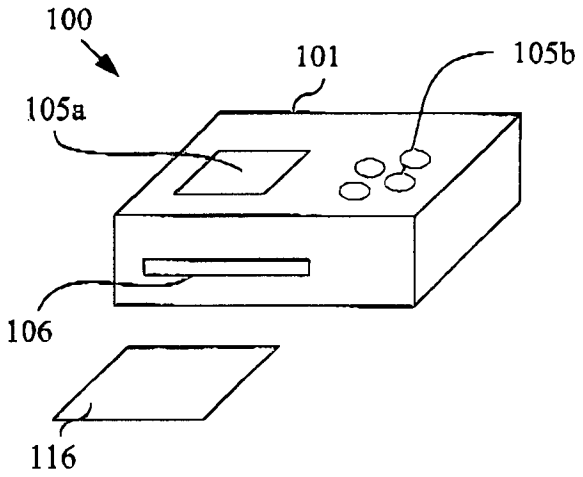

Fig. 3A

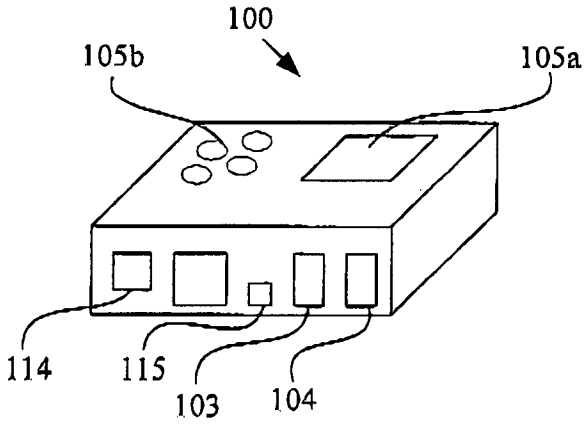

Fig. 3B

4646190525

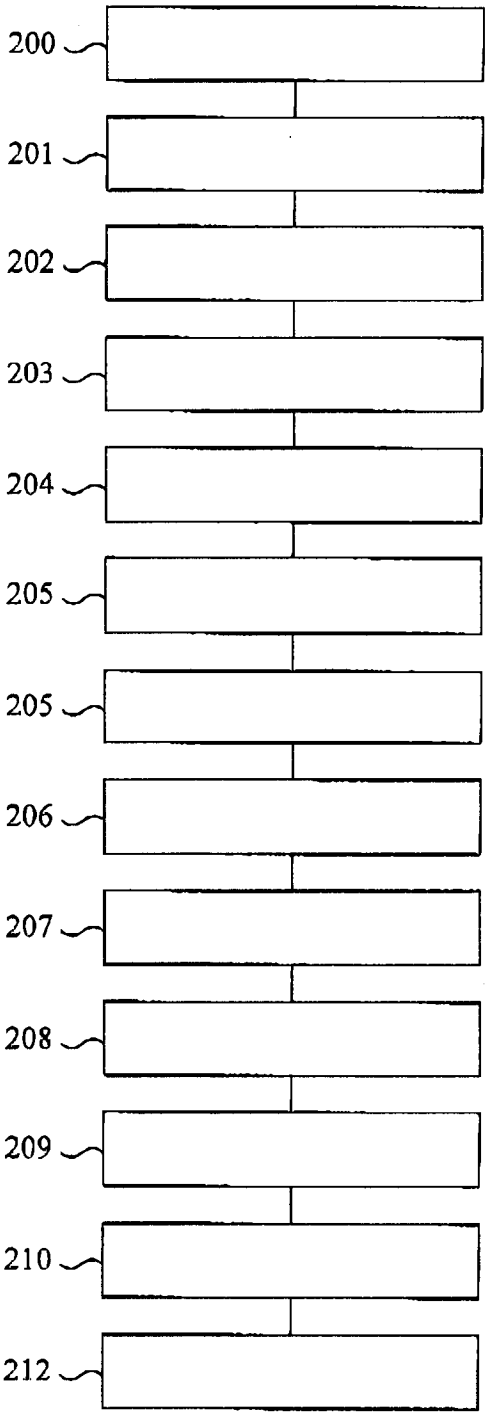

Fig. 4

4646190525

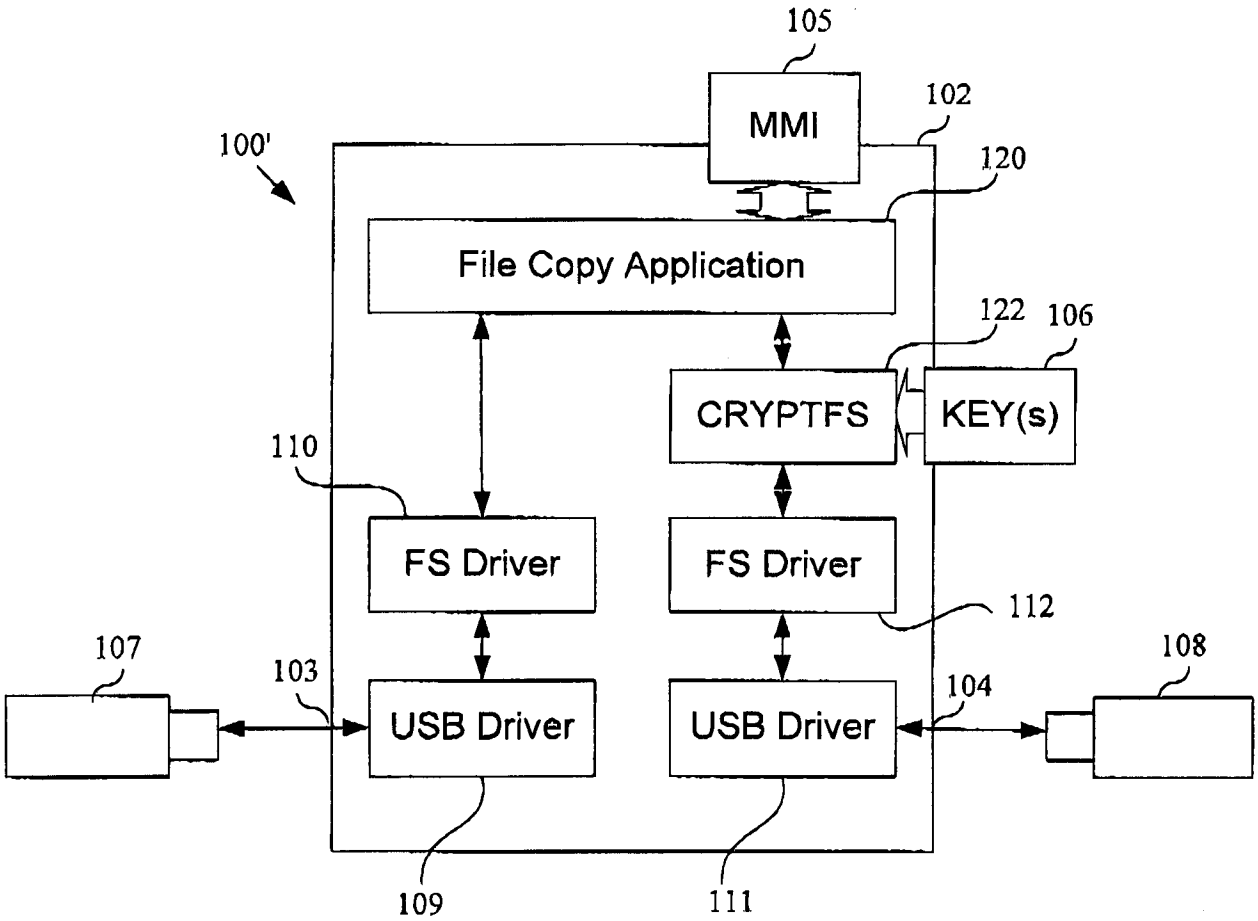

Fig. 5

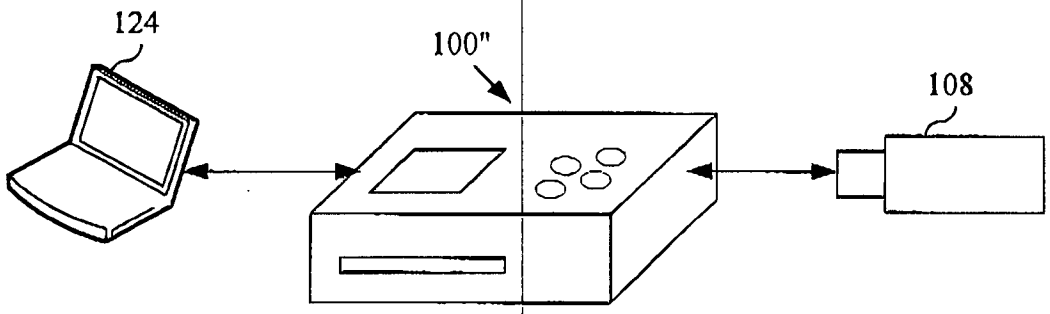

Fig. 6A

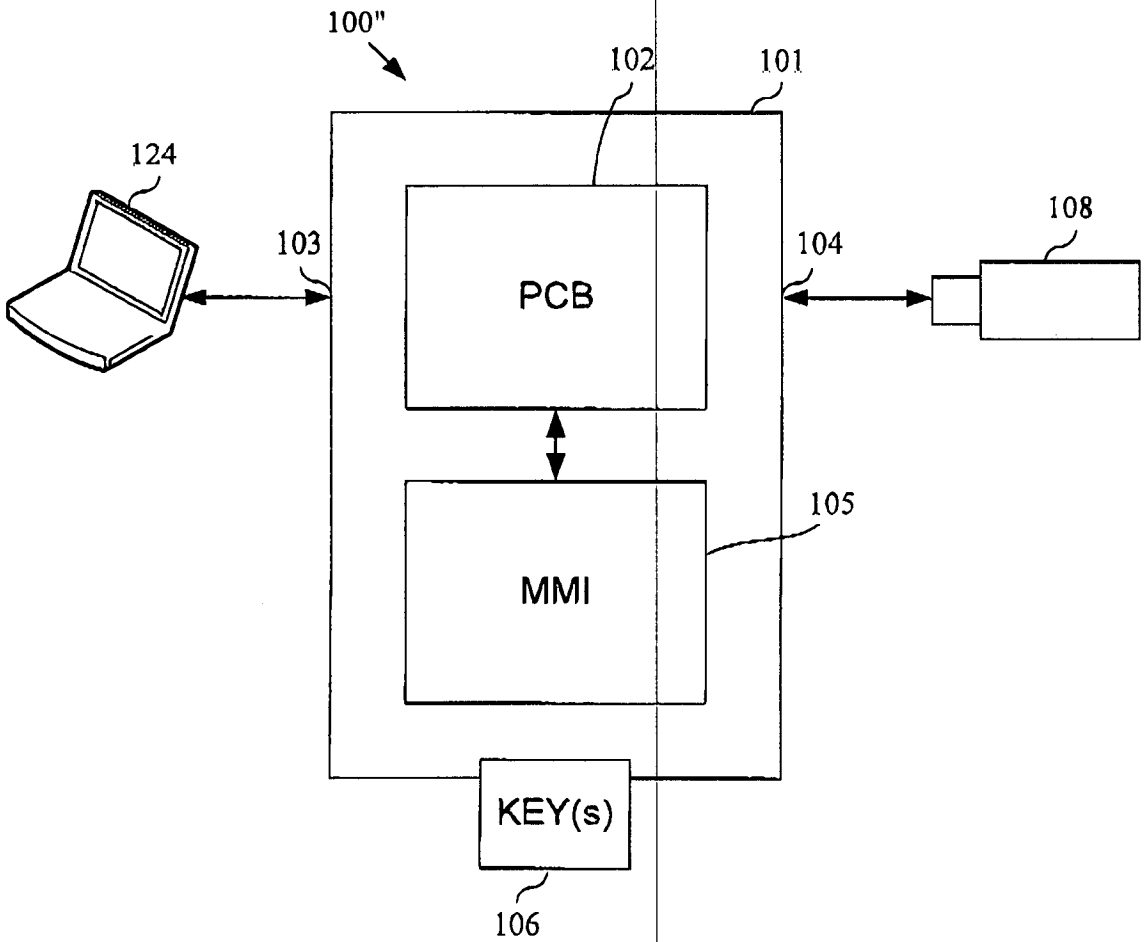

Fig. 6B

4646190525

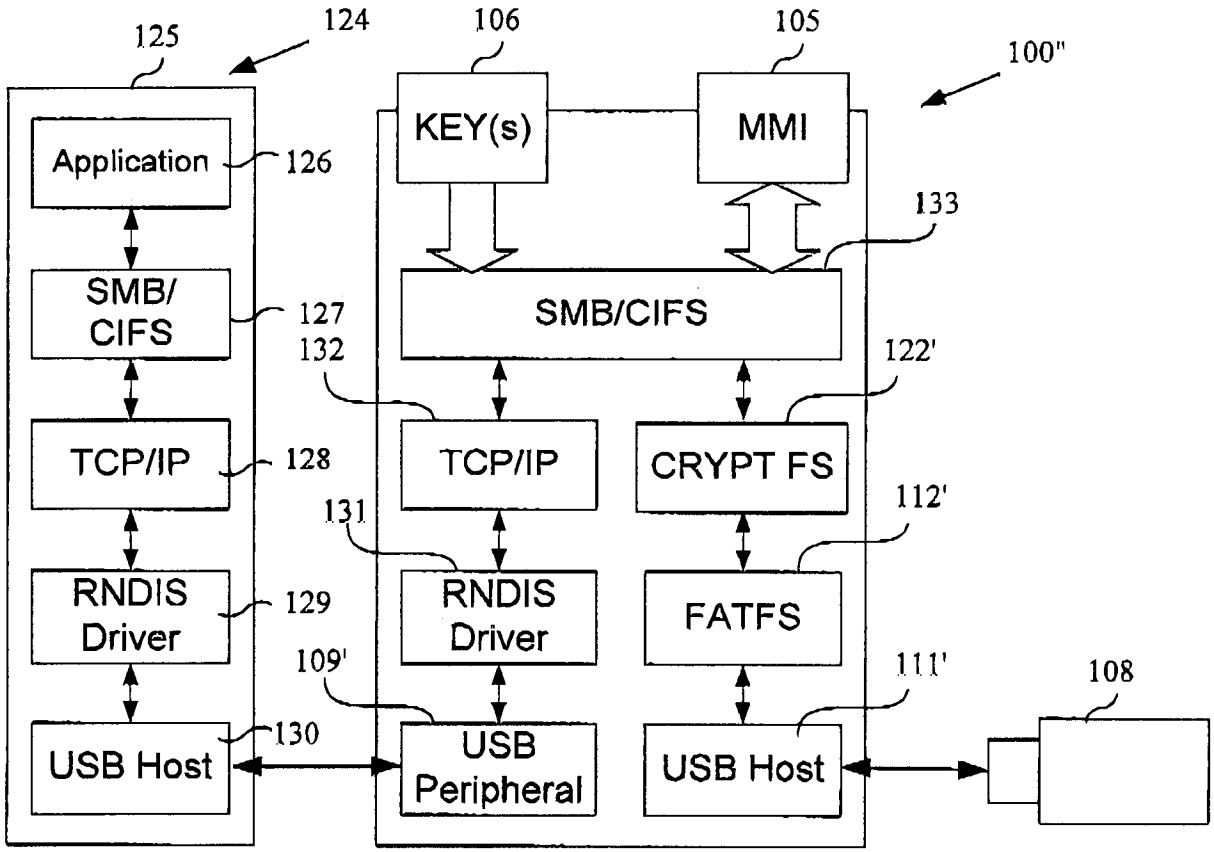

Fig. 7

4646190525

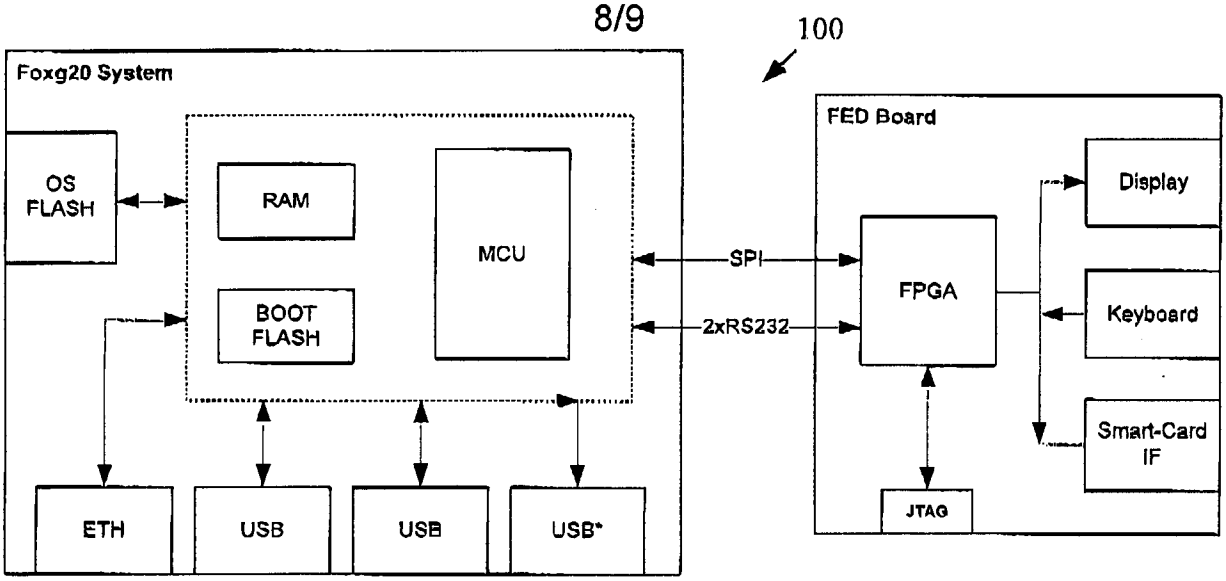

Fig. 8A

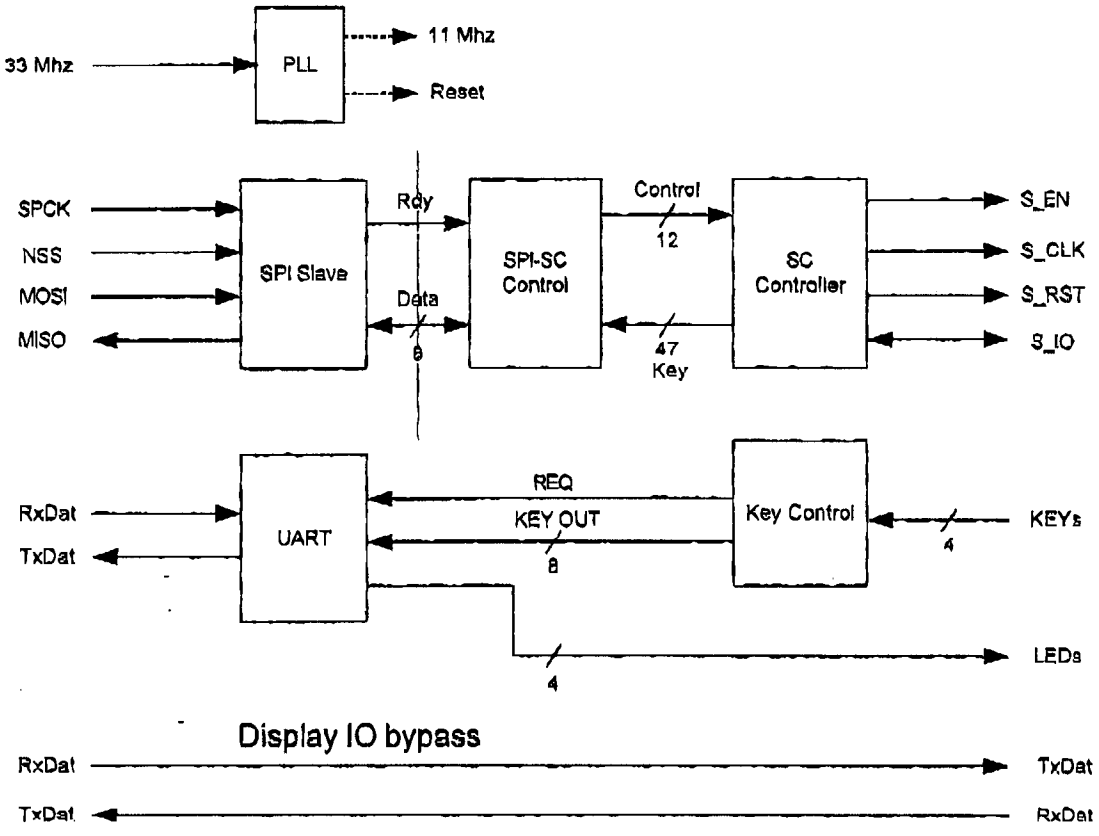

Fig. 8B

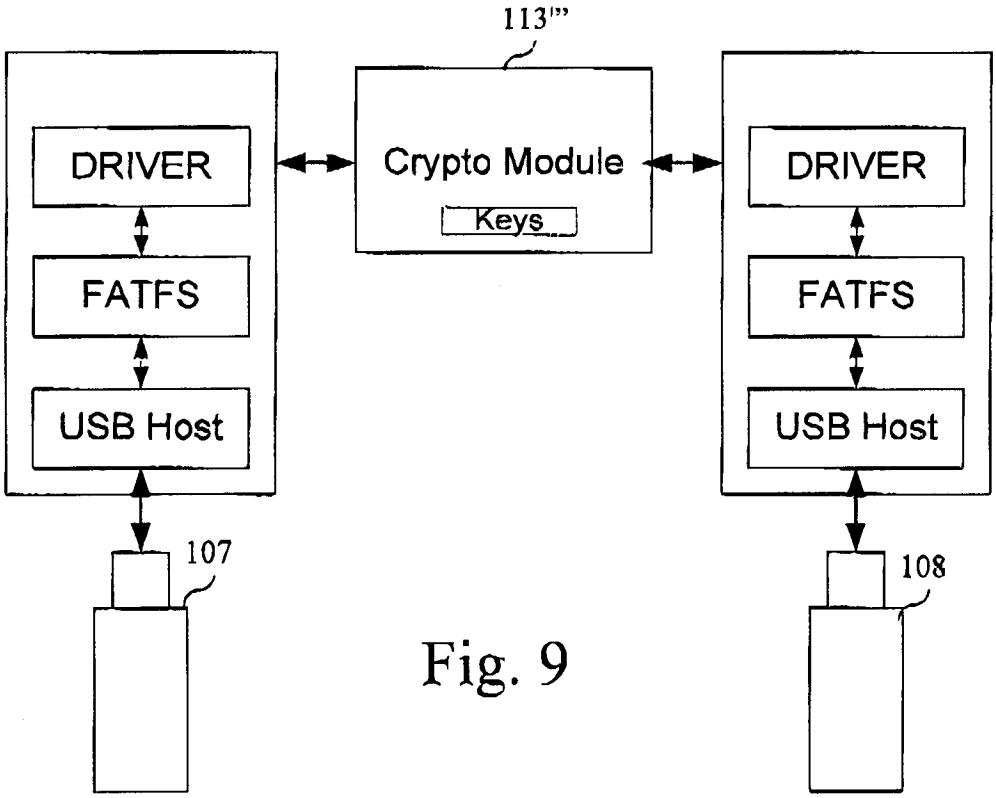
113'''
DRIVER
Crypto Module
Keys
DRIVER
FATFS
FATFS
USB Host
USB Host
107
108

Fig. 9

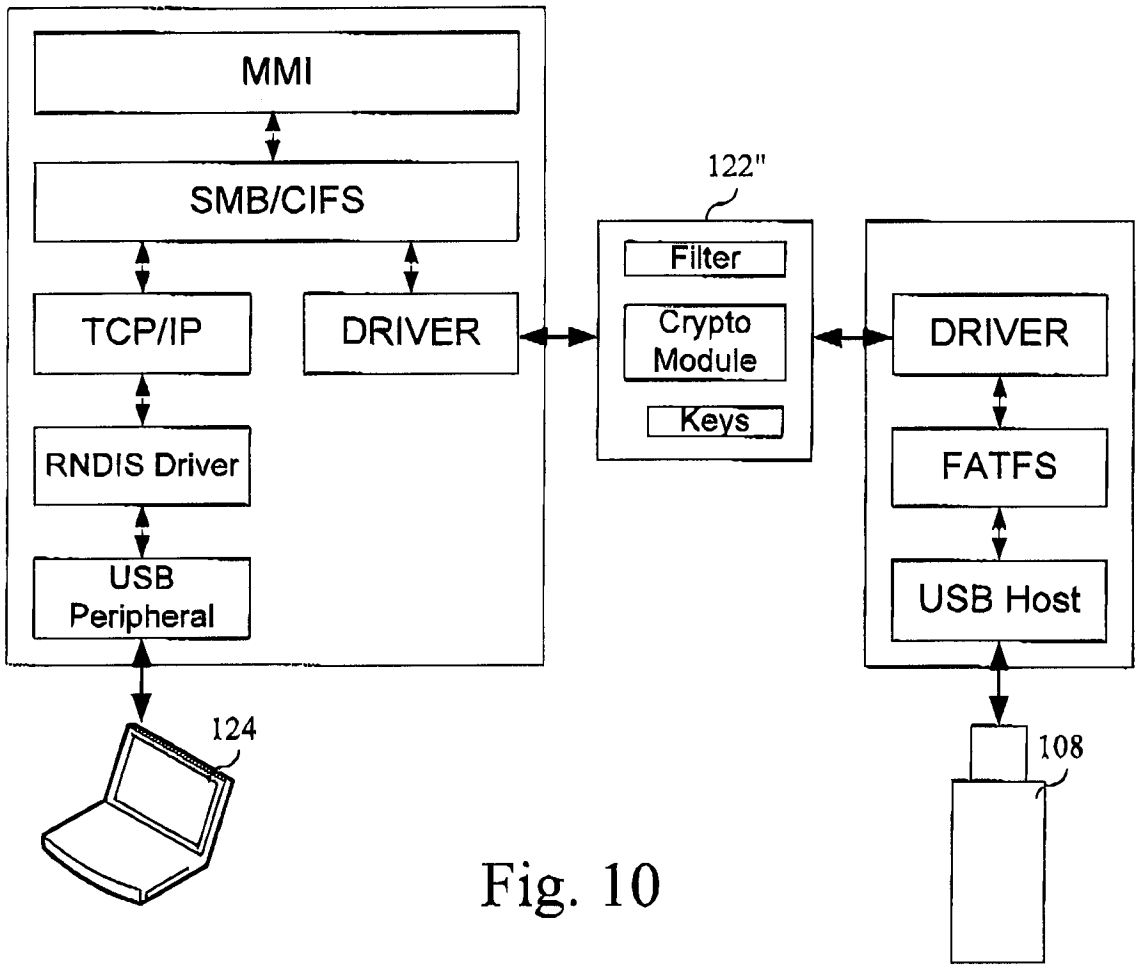
MMI
SMB/CIFS
122"
Filter
TCP/IP
DRIVER
Crypto Module
DRIVER
Keys
RNDIS Driver
FATFS
USB Peripheral
USB Host
124
108

Fig. 10