Greenliant®

MEMORY CARD AND MEMORY PROCESSING TECHNOLOGIES

A Patent Portfolio Acquisition Opportunity

Important Notice: The information contained in this and/or any other document, materials, or form of communication from the patent owner, **IP**investments Group, or its agents, now or in the future, related to the patent portfolio referenced herein (collectively, the "Information") is provided in connection with an offer for sale of the referenced patent portfolio. The Information does not constitute a legal analysis, opinion, or representation or warranty of any kind. The Information is provided solely to aid potential acquirers in conducting their own independent evaluation to determine whether to participate in the sales process conducted by **IP**investments Group. Any statement included in the Information regarding the potential use or applicability of any referenced patent or application to specific products or services is provided solely for illustration purposes and shall not be construed as notice of infringement or an accusation of infringement of any of the referenced patents. This document and/or any other document, materials, or communication is intended for receipt and review only by the parties (and their attorneys or agents) contacted by **IP**investments Group in connection with the sales process, and any redistribution beyond the receiving party's organization without **IP**investments Group's express written permission is strictly prohibited. **IP**investments Group reserves the right to suspend, discontinue, or modify the sales process at any time for any reason, in its sole discretion, without notice.

Memory Card and Memory Processing Technologies

A Patent Portfolio Acquisition Opportunity

Table of Contents

SECTION 1

Greenliant®

MEMORY CARD AND MEMORY PROCESSING TECHNOLOGIES

A PATENT PORTFOLIO ACQUISITION OPPORTUNITY

ACQUISITION OPPORTUNITY OVERVIEW

IPinvestments Group has been retained by Greenliant Systems, Ltd. to broker the sale of innovative mobile device memory cards and computing cache technologies (the "Portfolio"). The Portfolio provides higher capacity and security for multifunctional communication devices and/or memory cards (e.g., SIMS, etc.) with Internet connection capabilities and greater processing performance with a larger amount of non-volatile memory.

Also disclosed is a family of assets disclosing a pioneering memory and/or controller device that uses NAND flash memories to emulate the function of a NOR memory to replace the volatile DRAM or to be used as a bootable BIOS memory.

The Portfolio is currently being offered to select operating companies who participate in the relevant markets and related industries, as well as patent acquisition and financing organizations. The Portfolio is divided into four (4) distinct families that total three (3) issued U.S. Patents and seven (7) issued foreign patents. The Portfolio is best presented in two technical buckets as illustrated in the table below (the U.S. Patents are provided in the Appendix).

COUNTRY	PATENT NO.	TITLE	SERIAL NO.	FILING DATE	ISSUE DATE	PRIORITY DATE
BUCKET 1: MEMORY CARD RELATED TECHNOLOGIES:						
US	7,979,717	SECURE REMOVABLE CARD HAVING A PLURALITY OF INTEGRATED CIRCUIT DIES	12/100,400	04/09/08	07/12/11	04/09/08
US	8,200,281	SECURE REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE	12/502,897	07/14/09	06/12/12	07/14/09
KR	1,311,649	A SECURE REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE	20127003758	08/12/10	09/16/13	07/14/09
KR	1,018,170	A REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE	201015068	02/19/10	02/28/11	09/14/07
KR	1,035,468	A REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE	200866927	07/10/08	05/18/11	09/14/07
JP	5,015,112	A REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE	2008264613	09/11/08	08/29/12	09/14/07
CN	101,388,912	A REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE	200810149568	09/12/08	09/25/13	09/14/07
BUCKET 2: MEMORY PROCESSING TECHNOLOGIES:						
US	7,519,754	HARD DISK DRIVE CACHE MEMORY AND PLAYBACK DEVICE	11/637,419	12/11/06	04/14/09	12/28/05
TW	I317478	UNIFIED MEMORY AND CONTROLLER	2006147453	12/18/06	11/21/09	12/28/05
KR	797,325	UNIFIED MEMORY AND CONTROLLER	2006136568	12/28/06	01/16/08	12/28/05

EXAMPLE APPLICATIONS AND EMBODIMENTS OF THE PATENTED TECHNOLOGY:

The innovative memory technologies presented in the Portfolio are highly relevant to numerous industries and markets. As digital and/or computing systems increase in features, performance, and complexity, the need to manage the system interaction of non-volatile and volatile memories is growing more complex and new constraints are appearing. This is a strong and growing trend, especially in the mobile device market, as smartphones utilize SIM cards to secure and manage data.

Smartphones contain many systems with multiple controllers and/or processors, with both a baseband radio controller and an application processor that increase the complexity of the memory systems, processor access, and Internet and cellular network connections and authentication. While the patent portfolio is not limited to smart phones or mobile devices, smart phones are a prime and significant market where several of the patented technologies apply.

Today's mobile and computing systems are requiring ever larger amounts of storage (both removable and on hard disk drives), and therefore, the non-volatile memory of choice for higher density, NAND Flash, is increasingly being used. There is an imperative need for effective management and design of both volatile and non-volatile memory used in cards and modules as each technology favors certain functionality and specialized features from boot operations to multi-media storage and playback.

Heavy competition among manufacturers of memory solutions (i.e., cards, hard drives, ICs, etc.) is causing companies to look for innovation to aggressively shrink chip designs and free up related processing loads. The patented technologies enable features and mechanisms which provide greater control by mobile network operators (MNOs) and multiple service operators (MSOs) sending content to mobile devices that are connected to their network and provides for memory access from computing devices even when turned off.

The Portfolio includes numerous embodiments related to the patented technologies. Below are a few highlighted applications of some preferred embodiments that are in use today or are expected to be applied in the near future by many companies:

- SIM cards or other memory cards have increasingly been used to facilitate additional features related to Internet sessions. The memory cards may now be used to store secure information, such as passwords and financial data, etc.; which in turn is used to access or be provided during a session while connected to the Internet.

- The patented technologies present security to removable memory cards for communication devices where the non-volatile memory is presented in two portions. The first portion is restricted by the user but accessible by the carrier or service provider. The second portion is accessible by the carrier or service provider and through the processor to grant access to the user for storing encrypted data.

- The patented technology enables Internet access via the removable card as a cost effective solution. Typical SIM cards have been used by local servers to provide content to the cell phone; however, as taught in the Portfolio, the memory portion of the SIM card can be partitioned between a user restricted portion and a user accessible portion (and controlled via different modes), with the partition being alterable.

- A NOR emulating device that uses a controller and NAND memory in a computer system in place of the main memory or in place of the BIOS NOR memory. Therefore, the patented emulating device (memory or controller) can function as bootable memory. In addition, the device can act as a cache to the hard disk drive even when the power of the computing device is turned off or in hibernation.

THE PORTFOLIO

BUCKET 1: MEMORY CARD RELATED TECHNOLOGIES:

Just about every user of a hand held connected device (e.g., cell phones, smart devices, etc.) has had experience with some type of memory or subscriber identity module (i.e. SIM card). Typically, the memory is part of a removable card consisting of a processor, memory (e.g., RAM, ROM, EEPROM, Flash, etc.), I/O pads, and a security monitoring circuit. The non-volatile memory is used as secondary storage, or long-term persistent storage, to store required information to access the mobile phone operator’s network and services.

With increased speeds available in today’s 4G environment, the SIM card or other cards have increasingly been used to facilitate additional features related to Internet sessions. The SIM card may be used to store secure information, such as passwords and financial data, etc., used to access or during a session while connected to the Internet. Therefore, there is a need and demand for higher capacity and security for multifunctional communication devices and/or memory cards (e.g., SIMS, etc.) and greater processing performance with a larger amount of non-volatile memory.

Many of the patents in the Portfolio present innovative solutions for mobile devices and memory cards with the ability to connect to the Internet. The mechanisms introduced in the Portfolio for memory storage and Internet access through the mobile network are not costly or diminished and actually reduce the cost of accessing the Internet through a mobile network.

Some highlighted features include:

- Because the technology to manufacture high performance processors may not be compatible or optimal for manufacturing memory devices and controllers all integrated on the same die, the patented technologies present solutions for fabricating these devices on separate dies and integrating them via a bus and encrypted data exchange.

- As the cost of storage capacity continues to decrease, users have increasingly stored more valuable information including personal and private information in portable communication devices. Because these mobile devices can access the Internet, the provider of the common carrier service may offer the service of backing up that data on the Internet. Therefore, it is imperative to secure the data stored in portable mobile devices. Even if the user’s carrier provider does not offer Internet data backup services, users are wanting to secure the data, since the portable mobile device can easily be lost or stolen. The patented technologies present a removable card or a communication device where the non-volatile memory has two portions. The first portion is restricted by the user but accessible by the carrier or service provider. The second portion is accessible by the carrier or service provider and through the processor to grant access to the user for storing encrypted data.

- Today’s communication devices can access the Internet via a common carrier wireless network (such as a cellular network) and also access the Internet via a wireless link, such as a Wi-Fi link. However, accessing the Internet by the removable card is another cost effective solution. Typical SIM cards have been used by local servers to provide content to the cell phone; however, as taught in the Portfolio, the memory portion of the SIM card can be partitioned between a user restricted portion and a user accessible portion (and controlled via different modes), with the partition being alterable. Furthermore, the patented technologies enable features and mechanisms which provide greater control by mobile network operators (MNOs) and multiple service operators (MSOs) sending content to mobile devices that are connected to their network.

U.S. Patent No. 7,979,717 (the ‘717 Patent)

The ‘717 Patent is a standalone asset filed on April 9, 2008, and generally provides a removable card, such as, but not limited to, a SIM, with two integrated circuit dies working in tandem to provide encrypted communication to an external device or network. The ‘717 Patent provides the framework for an optimal memory card by fabricating different functions on separate dies and integrating the separate dies into a multichip module. This solution provides absolute security even if the card is removed and falls into the wrong hands.

U.S. Patent No. 7,979,717
Filed: 4/9/2008
Issued: 7/12/2011
Serial Number: 12/100,400

More specifically, the ‘717 Patent presents both system and methods for a secure removable card equipped with electrical connections for communication to outside devices or networks. The card comprises a first integrated circuit die that includes a processor. The card has a second integrated circuit die with non-volatile memory for storing a secret key, and a controller for controlling the operation of the non-volatile memory. The first die and the second die are connected by a bus.

The processor is enabled to generate a key pair, a public key portion and a private key portion upon power up, and transfers the public key portion across the bus to the second die. The controller receives the public key and encrypts the secret key with the public key and generates a first encrypted key, which is transferred across the bus to the first die. The processor receives the first encrypted key and decrypts the first encrypted key to recover the secret key; and is then able to encrypt data with the secret key for communicating along the electrical connections external to the card.

Representative Claim

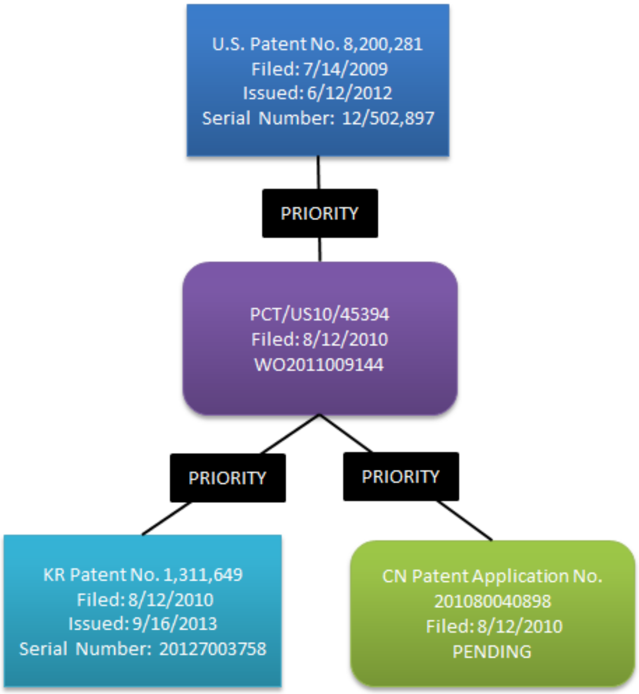
5. A method of securely communicating with a removable card, said card having electrical connections thereto and having a first semiconductor die, a second semiconductor die with an electrical bus connecting the first die with the second die, packaged together, said first die having a processor, said second die having a non-volatile memory for storing a secret key, and a controller for controlling the operation of the non-volatile memory, said method comprising:

generating a key pair, upon power up of the processor,
having a public key and a private key by the processor,
wherein said key pair generated is not based upon stored data;
transferring the public key to the second die via the electrical bus;
encrypting the secret key using the public key by the controller to produce an encrypted key;
transferring the encrypted key to the first die via the electrical bus;
decrypting the encrypted key to extract the secret key by the processor; and
using the secret key to encrypt data to communicate on the electrical connections external to the card.

NOTE: Claim No. 1 is a System claim that mirrors this method claim.

U.S. PATENT NO. 8,200,281 AND FOREIGN COUNTERPARTS (THE '281 PATENT FAMILY)

As illustrated in the below flow chart, the '281 Patent Family has a priority date of July 14, 2009, and generally provides proprietary technologies that enable and control the communication of mobile wireless devices with service providers through the Internet. The communication can occur through a memory card, such as a SIM card, or via a circuit module in the wireless communication device.



The '281 Patent Family presents a removable card with electrical connections used for connecting to a mobile wireless communicating device for users to access a carrier network and the Internet. The memory card comprises of a processor and a non-volatile memory connected to the processor. The non-volatile memory has two portions. The first portion is accessible by the provider of the carrier network with the processor restricting access by the user. The second portion is accessible by the provider of the carrier network and uses the processor to grant access to the user for storing user data therein. Furthermore, the removable card has logic circuit for encoding the user data to produce encrypted user data, for storing in the second portion. The logic circuit includes volatile memory for storing a user supplied password used when power is supplied. An encryption and decryption logic circuit receives the user supplied data and output from the volatile memory, to use the stored password, to produce user encrypted data and to decrypt user encrypted data.

Other claims focus not on a removable memory card, but on secured access to a mobile wireless communication device for use by a user to access a carrier network and Internet. The mobile device comprises a transceiver for communication wirelessly via a wireless carrier network. The mobile device further has a first processor for controlling communication of the device to connect to the common carrier network.

REPRESENTATIVE CLAIMS

1. A removable card having electrical connections for connecting to a mobile wireless communicating device for use by a user to access a common carrier network to access a network of interconnected computer networks (“Internet”), comprising:

a processor;

a non-volatile memory connected to the processor, having two portions: a first portion and a second portion wherein said first portion is accessible by the provider of the common carrier network with said processor restricting access thereto by the user, and wherein said second portion is accessible by the provider of the common carrier network and with said processor granting access thereto to the user for storing user data therein; and

logic circuit for encoding the user data to produce encrypted user data, wherein said encrypted data is stored in said second portion; wherein said logic circuit comprising a volatile memory for storing a user supplied password, wherein said password is stored in said volatile memory only when power is supplied to said memory;

an encryption circuit for receiving the user supplied user data and the output of the volatile memory and for encrypting said user data with said password from said volatile memory to produce encrypted user data, and for storing said encrypted user data in said second portion; and

a decryption circuit for receiving encrypted user data stored in the second portion and the output of the volatile memory and for decrypting said encrypted user data with said password from said volatile memory to produce user data.

5. A mobile wireless communication device for use by a user to access a common carrier network to access a network if interconnected computer networks (“Internet”) comprising:

a transceiver for communicating wirelessly via a wireless common carrier network;

a first processor for controlling communication of the device to connect to the common carrier network;

a second processor;

a non-volatile memory connected to the second processor, having two portions: a first portion and a second portion wherein said first portion is accessible by the provider of the common carrier network with said second processor restricting access thereto by the user, and wherein said second portion is accessible by the provider of the common carrier network and with said second processor granting access thereto to the user for storing user data therein; and

logic circuit for encoding the user data to produce encrypted user data for storing in said second portion;

wherein said logic circuit comprising a volatile memory for storing a user supplied password, wherein said password is stored in said volatile memory only when power is supplied to said memory;

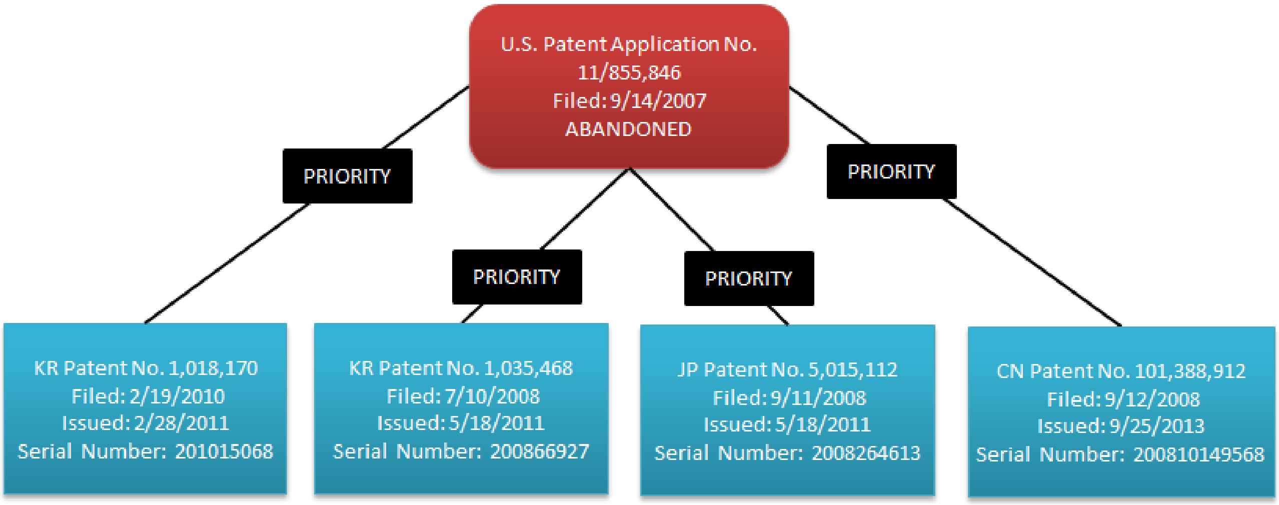
an encryption circuit for receiving the user supplied user data and the output of the volatile memory and for encrypting said user data with said password from said volatile memory to produce encrypted user data, and for

storing said encrypted user data in said second portion; and

a decryption circuit for receiving encrypted user data stored in the second portion and the output of the volatile memory and for decrypting said encrypted user data with said password from said volatile memory to produce user data.

FOREIGN PATENTS FAMILY (THE FOREIGN PATENT FAMILY)

The Portfolio contains related foreign patents (two Korean patents, One Japanese patent, and one Chinese patent) all with a priority date of September 14, 2007, from abandoned U.S. Patent Application No. 11/855,846. The relationships of these foreign issued patents are illustrated in the following flow chart.


U.S. Patent Application No. 11/855,846
Filed: 9/14/2007
ABANDONED

PRIORITY

KR Patent No. 1,018,170
Filed: 2/19/2010
Issued: 2/28/2011
Serial Number: 201015068

KR Patent No. 1,035,468
Filed: 7/10/2008
Issued: 5/18/2011
Serial Number: 200866927

JP Patent No. 5,015,112
Filed: 9/11/2008
Issued: 5/18/2011
Serial Number: 2008264613

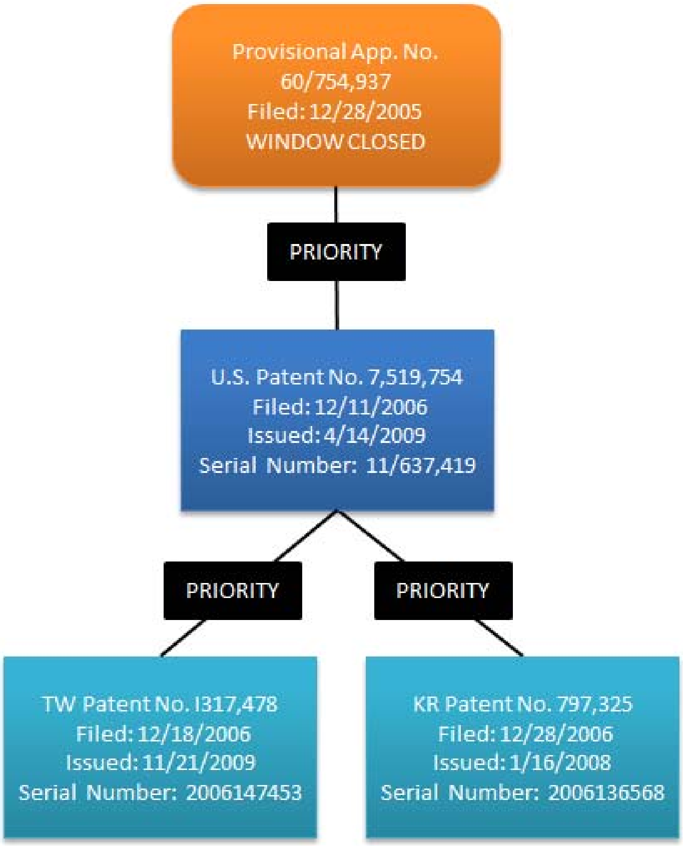
CN Patent No. 101,388,912
Filed: 9/12/2008
Issued: 9/25/2013
Serial Number: 200810149568

Generally, the Foreign Patent Family presents a removable card that has electrical connection to a device and has a processor and non-volatile memory connected to the processor. The non-volatile memory has programming code stored and configured to be processed by the processor to be operable in one of two modes. In a first mode, the card is connected to the device with the card storing information received wirelessly by the device from the Internet. In a second mode, the card is connected to a network portal device, which is connected to the Internet, with the card storing information received through the network portal device from the Internet.

BUCKET 2: MEMORY PROCESSING TECHNOLOGIES:

U.S. PATENT NO. 7,519,754 AND FOREIGN COUNTERPARTS (THE '754 PATENT FAMILY)

The '754 Patent Family has a priority date of December 28, 2005 from U.S. Provisional Application No. 60/754,937 (as illustrated in the below family relationship flow chart). Generally, the '754 Patent Family discloses memory caching technologies for personal computers where memory and controller devices use NAND flash memories to emulate the function of NOR memory. The patented technologies can function as a playback device for music or videos via use of the hard drive while a computer or laptop is powered off or in hibernation mode.



The patented NOR emulating device uses a controller and NAND memory in a computer system in place of the main memory or in place of the BIOS NOR memory. Therefore, the emulating device (memory or controller) can function as bootable memory. In addition, the device can act as a cache to the hard disk drive. With the addition of an MP3 player controller into the device, the device can function as a standalone audio playback device, even while the PC is turned off or is in a hibernating mode. As an audio MP3 player controller, the patented device can access additional audio data stored on the hard drive, with the computing device (e.g., PC, laptop, tablet, smartphone, etc.) in an off mode or a hibernating mode.

As mentioned above, the pioneering memory device uses NAND flash memories to emulate the function of a NOR memory to replace the volatile DRAM or to be used as a bootable BIOS memory. In addition, the memory device can act as a cache to the hard disk drive and the memory device can act as a hub for USB devices, thereby controlling the transfer of data to/from the hard disk drive, even while power is off to the main processor.

Since the memory device has a controller it can perform other functions (or a dedicated processor, such as DSP, can also be used) such as for MP3 playback. Therefore, the memory device can function as a standalone audio playback device and can access additional audio data stored on the hard drive, even while the computing device is turned off or is in a hibernating mode.

REPRESENTATIVE CLAIMS

1. A controller circuit comprising:
a first plurality of ports for connecting to a first plurality of buses for receiving and providing signals therefrom, and a second plurality of ports for connecting to a second plurality of buses for receiving and providing signals therefrom;
a third port for connecting to a memory;
said controller circuit operable in one of two modes: wherein in a first mode, said controller circuit functions as pass through device to provide signals transparently to and from the plurality of first buses to the plurality of second buses; and wherein in a second mode, said controller circuit functions to monitor signals from one of the second plurality of buses to another of said second plurality of buses, in response to said signals requesting data from said controller circuit wherein said controller circuit analyzes said signals to determine if said data is in said memory.

NOTE: Claim No. 2 mirrors the above claim but "traps" the signals instead of "monitor."

5. A memory device comprising:
a first plurality of ports for connecting to a first plurality of buses for receiving and providing signals therefrom, and a second plurality of ports for connecting to a second plurality of buses for receiving and providing signals therefrom;
said memory device operable in one of two modes: wherein in a first mode, said memory device functions as a pass through device to provide said signals transparently to and from the plurality of first buses from and to the plurality of second buses; and wherein in a second mode, said device functions to monitor said signals from one of the second plurality of buses directed to one of said first plurality of buses, wherein said signals request data from said one of said first plurality of buses, and wherein said memory device serves to respond to said signals in the event said data requested is in said memory device.

NOTE: Claim No. 6 mirrors the above claim but "traps" and "re-transmits" the signals instead of "monitor" and "respond."

SECTION 2

IPINVESTMENTS GROUP

The Forum, Suite 140
3930 E. Jones Bridge Road
Atlanta, Georgia 30092

Main: (404) 962-8740
Fax: (404) 962-8741
www.ipinvestmentsgroup.com

IPinvestments Group is an intellectual property business advisory firm committed to extracting maximum value for intellectual property assets. IPinvestments Group provides transactions and licensing services related to the selling and/or licensing of patented technologies. More specifically, we are intellectual property investment brokers who market, auction and/or sell patents on behalf of the patent owner. In addition to transactions, we assist our clients and partner in the development, implementation and management of patent licensing programs.

Determining the fair market value of intellectual property is critical to evaluating potential technology transactions. Our professionals have a tremendous amount of experience valuing intellectual property and determining reasonable royalties for intellectual property across a broad range of technologies and industries.

IPinvestments Group's professionals have backgrounds in accounting, engineering, finance and IP law, as well as extensive experience in negotiating the economics of intellectual property rich transactions and license agreements. We perform our intellectual property transactions and licensing work under a "success fee" structure (a/k/a – contingency fee). We have been engaged by Fortune 500 companies, government agencies, universities, privately held companies, investment / financial firms, and individuals.

Please direct any questions or inquiries to:

William A. Hartselle
Principal
Direct Line – (404) 962-8744
bhartselle@ipinvestmentsgroup.com

Charles W. Chamberlain
Sr. Director
Direct Line – (404) 962-8739
cchamberlain@ipinvestmentsgroup.com

APPENDIX

APPENDIX
TAB A

US007979717B2

(12) **United States Patent**
Ding

(10) **Patent No.: US 7,979,717 B2**
(45) **Date of Patent: Jul. 12, 2011**

(54) **SECURE REMOVABLE CARD HAVING A PLURALITY OF INTEGRATED CIRCUIT DIES**

(75) Inventor: **Zhimin Ding**, Sunnyvale, CA (US)

(73) Assignee: **Greenliant LLC**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 655 days.

(21) Appl. No.: **12/100,400**

(22) Filed: **Apr. 9, 2008**

(65) **Prior Publication Data**

US 2009/0257590 A1 Oct. 15, 2009

(51) **Int. Cl.**
G06F 21/00 (2006.01)
H04M 1/00 (2006.01)

(52) **U.S. Cl.** **713/185**; 726/9; 726/20; 455/558

(58) **Field of Classification Search** 726/9, 20; 380/44–47, 277–286; 713/185; 455/558
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,581,841	B1 *	6/2003	Christoffersen	235/492
2002/0023963	A1 *	2/2002	Luu	235/492
2002/0026578	A1 *	2/2002	Hamann et al.	713/159
2003/0135731	A1 *	7/2003	Barkan et al.	713/155
2005/0120205	A1 *	6/2005	Umezawa et al.	713/156
2006/0172573	A1 *	8/2006	Laitinen et al.	439/159
2008/0016352	A1 *	1/2008	Perlman	713/171
2008/0080255	A1 *	4/2008	Kagan et al.	365/185.23
2009/0075698	A1 *	3/2009	Ding et al.	455/558
2009/0121028	A1 *	5/2009	Asnaashari et al.	235/492
2009/0121029	A1 *	5/2009	Asnaashari et al.	235/492
2009/0122989	A1 *	5/2009	Asnaashari et al.	380/278
2010/0023747	A1 *	1/2010	Asnaashari et al.	713/150

OTHER PUBLICATIONS

Posegga, "The WebSIM: Smartcard Goes Internet," Joachim. Posegga@Telekom.de, Jan. 31, 2000, 2 pages.
Gemalto, "dot-sim, How a little dot can have a big impact on your business" Telecom Marketing & Strategy Team, Jul. 2006, pp. 1-18.
Guthery, et al., "How to Turn A GSM SIM Into A Web Server," Submitted for CARDIS 2000., pp. 1-13.
Rees, et al., "Webcard: A Java Card Web Server," CITI Technical Report 99-3., Oct. 1, 1999, pp. 1-6.
U-M Develops the World's Smallest Web Server in Partnership With Schlumberger, Univ. of Michigan News Service., Oct. 27, 1999, pp. 1-2.

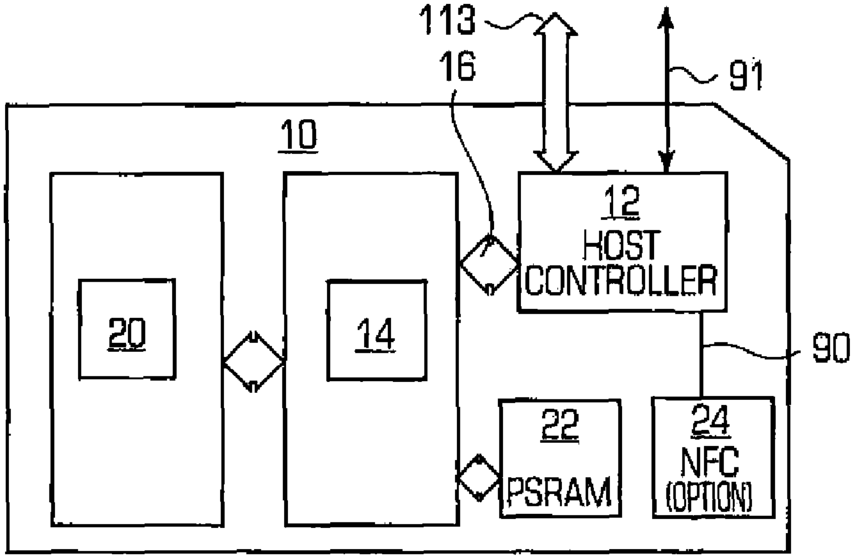
(Continued)

Primary Examiner — Christian LaForgia
(74) *Attorney, Agent, or Firm* — DLA Piper LLP (US)

(57) **ABSTRACT**

A secure removable card has electrical connections for communication therewith. The card comprises a first integrated circuit die, with the first die including a processor. The card has a second integrated circuit die, with the second die including a non-volatile memory for storing a secret key, and a controller for controlling the operation of the non-volatile memory. A bus connects the first die with the second die. The processor can generate a key pair, having a public key portion and a private key portion upon power up, and transfers the public key portion across the bus to the second die. The controller can receive the public key and encrypt the secret key with the public key to generate a first encrypted key, and can transfer the first encrypted key across the bus to the first die. The processor can receive the first encrypted key and can decrypt the first encrypted key to recover the secret key, and can encrypt data with the secret key for communicating along the electrical connections external to the card.

9 Claims, 3 Drawing Sheets



OTHER PUBLICATIONS

Monroe, “World’s Smallest Web Server A Partnership Project,” The University Record., Dec. 13, 1999. pp. 1-2.
Ito, et al., “Secure Internet Smartcards,” Lecture Notes in Computer Science, Springer Berlin/Heidelberg, vol. 2041, 2001, pp. 1-2.
“Oberthur Card Systems Enables SIM Cards to Host Operator’ Web Portals,” Oberthur Card Systems, pp. 1-2.
Chan, “Web-Enabled Smart Card For Ubiquitous Access Of Patient’s Medical Record,” Internet Computing And Electronic Commerce Laboratory, Dept. of Computing, The HongKong Polytechnic Univ., Hung Hom, Kowloon, HongKong, pp. 1-10.
“Internet Smart Card, security2go—WebServer,” Giesecke & Devrient, 2007, pp.1-2.
Balaban, “Can Web-Server Card Brighten A Drab SIM?” CardTechnology.com and SourceMedia, Inc., 2007, pp. 1-5.
Jackson, “Cards Get Smarter,” Government Computer News, May 2007, pp. 1-2.
8th Edition e-Smart Conference & Demos 2007, Sep. 2007, Sophia Antipolis, French Riviera, 4 pages.
Lenhart, “The Smart Card Platform,” ETSI Technical Committee Smart Card Platform (TB SCP), 26 pages.

* cited by examiner

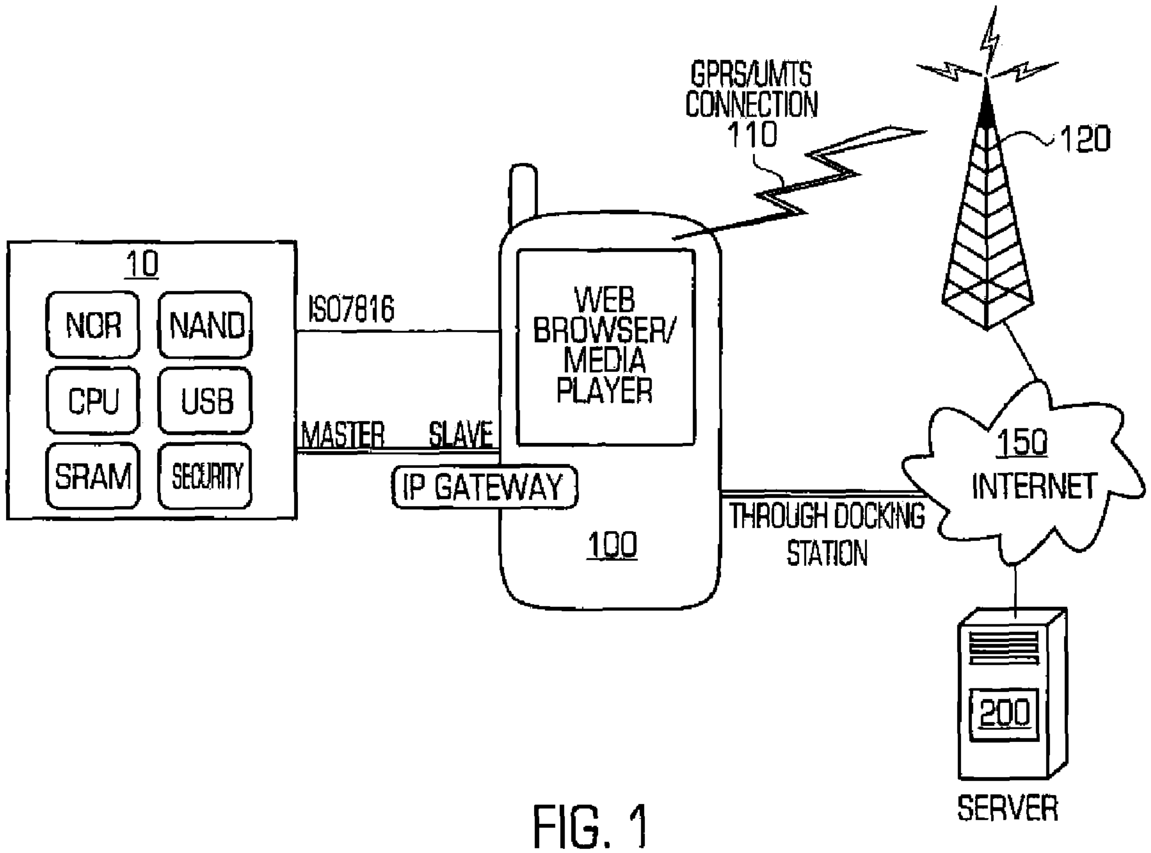


FIG. 1

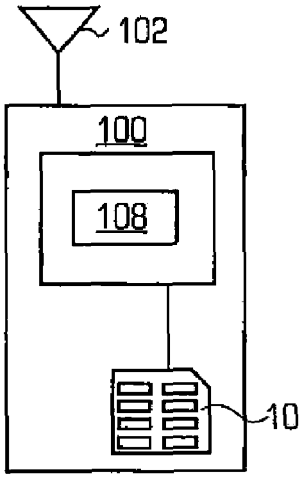


FIG. 2

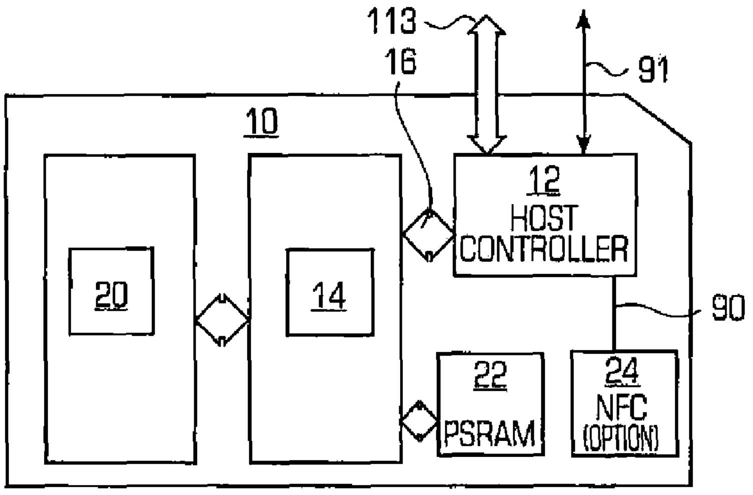


FIG. 3

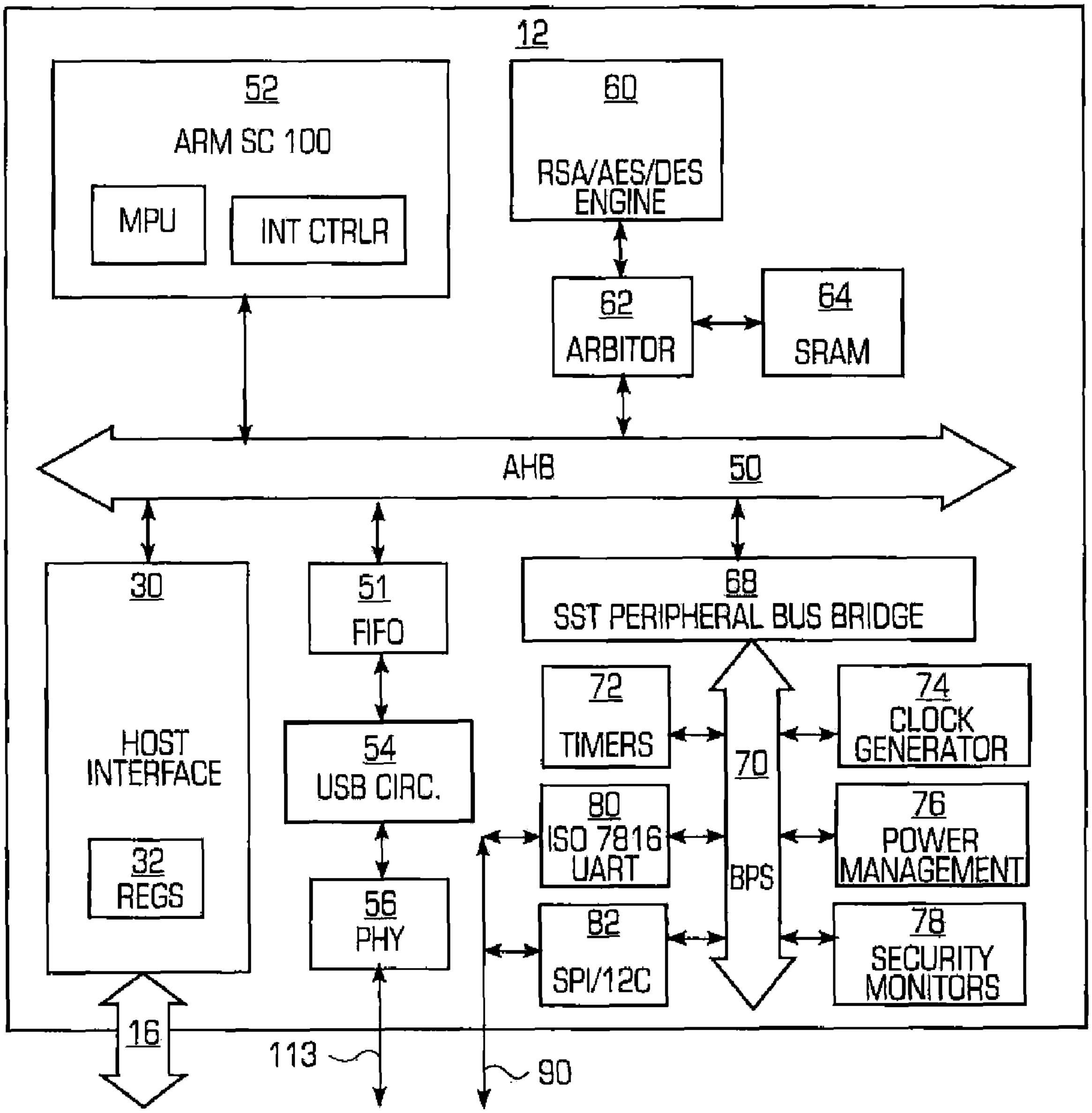

12
52
ARM SC 100
MPU
INT CTRLR
60
RSA/AES/DES ENGINE
62
ARBITOR
64
SRAM
AHB
50
30
HOST INTERFACE
32
REGS
51
FIFO
54
USB CIRC.
56
PHY
68
SST PERIPHERAL BUS BRIDGE
72
TIMERS
70
BPS
74
CLOCK GENERATOR
80
ISO 7816 UART
76
POWER MANAGEMENT
82
SPI/12C
78
SECURITY MONITORS
16
113
90

FIG. 4

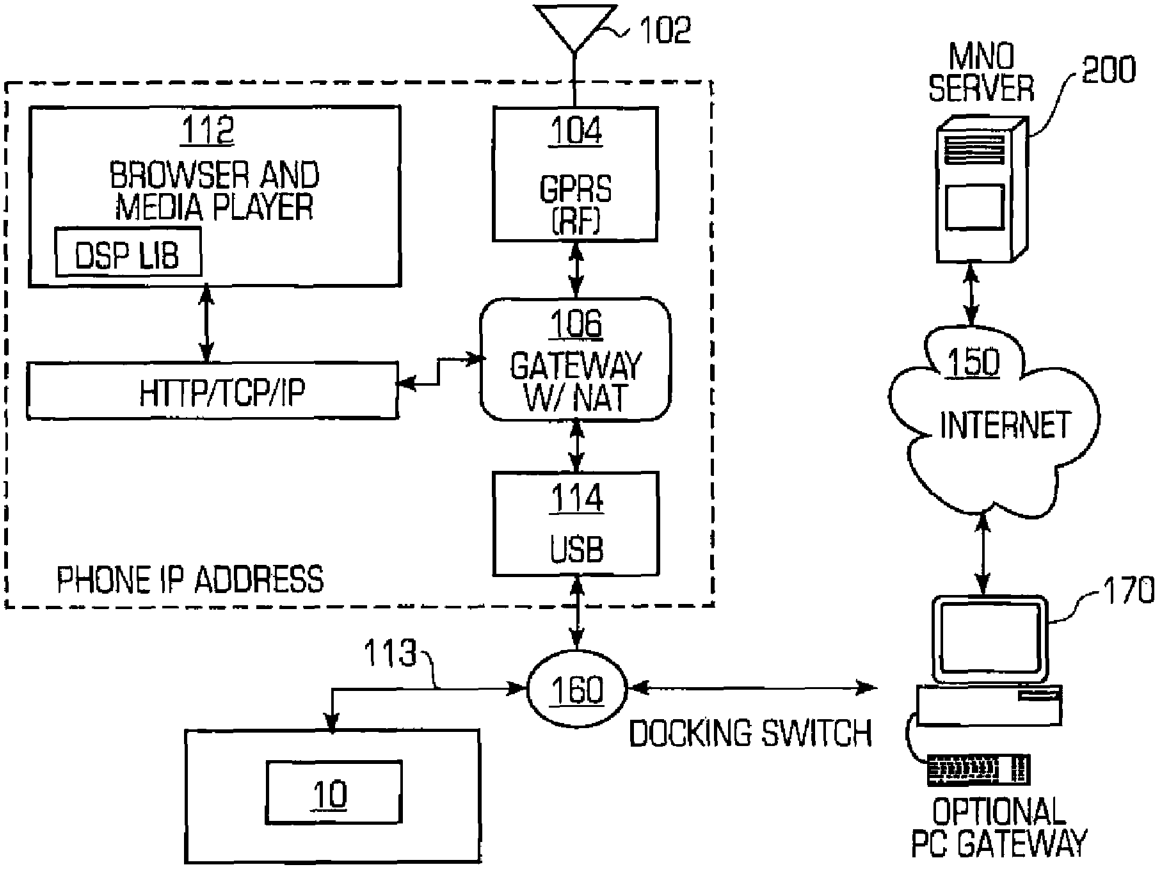

102
112
BROWSER AND MEDIA PLAYER
DSP LIB
104
GPRS (RF)
106
GATEWAY W/ NAT
HTTP/TCP/IP
114
USB
PHONE IP ADDRESS
113
160
DOCKING SWITCH
10
MNO SERVER
200
150
INTERNET
170
OPTIONAL PC GATEWAY

FIG. 5

SECURE REMOVABLE CARD HAVING A PLURALITY OF INTEGRATED CIRCUIT DIES

TECHNICAL FIELD

The present invention relates to a secure removable card having a plurality of integrated circuit dies, one of which contains a non-volatile memory for storing a secret key, wherein the card is secure from probing.

BACKGROUND OF THE INVENTION

Mobile wireless communication devices, such as cell phones are well known in the art. Typically, a cell phone has a removable card (called "SIM card") which consists of a processor with RAM, ROM or EEPROM or Flash memory, I/O pads, and security monitoring circuit all mounted on a removable card. The non-volatile memory in the SIM card is to store information required to access the mobile operator's network. Thus, the card may store information such as telephone number, access code, number of minutes, calling plan etc.

A network of interconnected computer networks ("Internet") is also well known in the art. The Internet can be accessed by computers having a wired connection, or through a wireless network.

With the increase in speed in mobile networks, such as the 3G network, users of mobile wireless devices desire to access the Internet via their mobile wireless communication devices.

Thus, increasingly, the SIM card may be used to store secure information such as passwords, financial data etc. used to access the Internet or during a session on the Internet.

Therefore, there is increasing demand for higher capacity SIM cards that include a higher performance processor and larger amount of non-volatile memory. However, since the technology to manufacture high performance processors may not be compatible or optimal for manufacturing of memory devices or memory controller devices, integrated on the same die, there is a need to fab these devices on separate dies and to integrate the dies into a multichip module. Hence it is desirable to provide a mechanism whereby these types of information are secure even if the removable card falls into the wrong hands.

SUMMARY OF THE INVENTION

Accordingly, in the present invention, a secure removable card has electrical connections for communication therewith. The card comprises a first integrated circuit die, with the first die including a processor. The card has a second integrated circuit die, with the second die including a non-volatile memory for storing a secret key, and a controller for controlling the operation of the non-volatile memory. A bus connects the first die with the second die. The processor can generate a key pair, having a public key portion and a private key portion upon power up, and transfers the public key portion across the bus to the second die. The controller can receive the public key and encrypt the secret key with the public key to generate a first encrypted key, and can transfer the first encrypted key across the bus to the first die. The processor can receive the first encrypted key and can decrypt the first encrypted key to recover the secret key; and can encrypt data with the secret key for communicating along the electrical connections external to the card.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a diagram of the removable card of the present invention connected to a mobile wireless communication device of the present invention for connection to a mobile network, as well as to the Internet.

FIG. **2** is a schematic diagram of the removable card of the present invention connected to the mobile wireless communication device of the present invention.

FIG. **3** is a block level diagram circuit diagram of the removable card of the present invention.

FIG. **4** is a detailed circuit diagram of the processor portion of the removable card of the present invention.

FIG. **5** is a diagram of the two modes of communication of the mobile wireless communication device with the removable card of the present invention with the Internet, wherein in the first mode, the removable card communicates through the wireless communication device wirelessly with the mobile network for access to the Internet, and wherein in a second mode the removable card is connected to a network portal device for connection to the Internet.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to FIG. **1** there is a shown a graphic illustration of a mobile wireless communication device **100**, e.g. a cell phone **100** for use in a publicly accessible (common carrier) wireless communication network, such as a cellular network **110**, which includes cellular access towers **120**. The cellular network **110**, through access servers (not shown) located on or near the cell phone towers **120** can connect to a network of interconnected computer networks **150**, also known as the Internet **150**. Thus, the cell phone **100** can communicate wirelessly with other cell phones **100** on the cell phone network **110**. In addition, the cell phone **100** can communicate wirelessly with the Internet **150** through the cell phone network **110** which has the access servers connected to the Internet **150**. Further, as will be shown hereinbelow, the removable card **10** portion of the cell phone **100** can also be connected directly to the Internet **150** through a network portal device, such as docking station **160**, which is connected to a personal computer, which connects to the Internet **150**.

The cell phone **100** of the present invention has a removable card **10**, much like the removable SIM card of the prior art. However, as will be seen, the features of the removable card **10** of the present invention are vastly different and improved over the removable SIM card of the prior art. As a result, the removable card **10** of the present invention is called a SIM module.

Referring to FIG. **2**, there is shown a schematic diagram of the removable card **10** of the present invention connected to the mobile wireless communication device **100** of the present invention. Because the device **100** is designed to operate wirelessly across the cellular network **110**, the device **100** comprises an antenna **102**. A transceiver **104** is connected to the antenna **102**. The transceiver **104** transmits and receives modulated signals to and from the cellular network **110**. Such components are well known in the art. The received signals may be demodulated and then converted into digital signals and provided to a gateway **106**. The gateway **106** may also have an NAT (Network Address Translation) circuit. An NAT circuit **106** translates or maps a private IP address to one or more ports of a public IP address. As will be discussed hereinafter, the device **100** (through the removable card **10**), may be assigned a public address (through the well known DHCP protocol) when the device is connected to the Internet **150**, and may have a private address when operating as a local server such that the device **100** is not connected to the Internet **150**. Digital signals to be transmitted are modulated and converted by the transceiver **104** into appropriate electromagnetic frequency signals for transmission by the antenna **102**. Because the device **100** can access the Internet **150**, a browser and media player **112** is also provided. The browser and media player **112** interfaces in the well known TCP/IP protocol as well as the HTTP protocol with the gateway **106** to provide and to receive digital signals received by the device **100** from the Internet **150**, which may be displayed on a display **108**. Associated with the browser and media player **112** is a processor (not shown) which also controls the transceiver **104** and other well known hardware circuits of the device **100** to communicate with the network **110**.

The removable card **10** of the present invention is connected to the device **100** through a well known USB interface **114** through the docking station **160**. The USB interface **114** connects to the Gateway **106**. Thus, digital signals from the removable card **10** are provided to and from the device **100** through the docking station **160**, through the USB interface **114**, through the gateway **106** and through the transceiver **104** to the antenna **102**.

The removable card **10** of the present invention is shown in greater detail in FIG. **3**. in particular, the card **10** comprises a host controller **12** which interfaces with the USB interface **114** through a USB bus **113**. In addition, the host controller **12** is connected to a memory controller **14**, through a bus **16**. The memory controller **14** controls a NAND memory **20** and a PSRAM **22**. The operation of the memory controller **14** in controlling the NAND memory **20** and the PSRAM **22** is fully described in U.S. patent application Ser. No. 11/637,420, published on Jun. 28, 2007 under publication 2007-0147115, and assigned to the present assignee, which disclosure is incorporated by reference herein in its entirety. The host controller **12** may also be optionally connected to a Near Field Communicator (NFC) **24**. An NFC **24** is a close range RF circuit that permits wireless communication in close proximity. Thus, the device **100** with the NFC **24** may act as an "electronic wallet" for financial transactions or for identification purpose, or as another access to the Internet **150**. Of course, the device **100** can also be connected wirelessly with the Internet **150** via other forms of wireless networks, such as a Wi-Fi network.

Referring to FIG. **4**, there is shown a detailed schematic block diagram of the host controller **12**. The host controller **12** comprises a high speed bus **50**, to which a host interface **30**, for connecting to the memory controller **14** is attached. The host interface **30** also comprises registers **32** for temporarily holding data that is supplied to and from the memory controller **14**. The host controller **12** also comprises a FIFO (First-In First Out) circuit **51** which is connected to the high speed bus **50**. The FIFO **51** is also connected to a USB controller circuit **54**, which is connected to a PHY circuit **56** (which is the standard physical layer interface for a USB port. The circuit **56** includes pads, voltage level shifters and clock recovery circuits.) for connection to the USB bus **113**. A secure processor, such as an ARM SC-100 processor **52** is also connected to the high speed bus **50**.

The host controller **12** also comprises a RSA/AES/DES engine **60**, which is a secure co-processor to the ARM SC-100 processor **52**. The engine **60** is connected to the high speed bus **50** through an arbitration circuit **62**. Since both the engine **60** and the processor **52** can request memory or other resources of the high speed bus **50** at the same time, the arbitration circuit **62** arbitrates simultaneous requests for access to the bus **50**. The engine **60** also has access to a dedicated high speed cache RAM, such as an SRAM **64**. Finally, a bridge circuit **68** is also connected to the high speed bus **50**. The bridge circuit **68** is also connected to a slower bus **70**, to which a timer **72** is connected, a clock generator **74** is connected, a power management circuit **76** is connected, a security monitoring circuit **78** is connected, a UART **80** is connected, and a SPI circuit **82** (Serial Peripheral Interface—a well known bus) is connected. The UART **80** and the SPI **82** are also connected to a bus **90**, which is connected to the NFC **24**. The controller **12** is also connected to a bus **91** which is a ISO7816 serial interface bus. It is a byte oriented Universal Asynchronous Receiver/Transmitter (UART) interface commonly found in prior art cell phones between the phone and the SIM card. This type of interface (using UART) is being replaced by the USB interface. Thus, the presence of the bus **91** is for backward compatibility only.

Operation of the Mobile Wireless Communication Device

There are many modes of operation of the mobile wireless communication device **100** of the present invention. Initially, it should be noted that the mobile network operator (MNO), the operator of the cellular network **110**, distributes each of the removable cards **10**, and also has a server **200** connected to the Internet **150**. Each of the removable cards **10** of the present invention distributed by the MNO is assigned a unique public IP address by the MNO which is stored in the non-volatile memory portion of the removable card **10**. The unique public IP address directs the device **100** to the MNO server **200**. As disclosed in U.S. patent application Ser. No. 11/637,420, published on Jun. 28, 2007 under publication 2007-0147115, non-volatile memory is present in the NAND memory **20** as well as NOR memory being embedded in the controller **14**. In either event, the MNO assigns and pre-stores a unique public IP address in the non-volatile memory portion of the removable card **10**. The non-volatile memory may be divided into two portions, with the partition between the first portion and the second portion being alterable. The partitioning of the first portion/second portion can be done by the MNO provider of the removable card **10**. The first portion can be accessed by the processor which controls the transceiver **104** and browser and media player **112**, and the other hardware circuits that control the communication of the device **100**. The second portion can be accessed by the processor **52**, in the removable card **10**, which is accessible by the user. In addition, the processor **52** controls the degree of access (which includes the type of information) that a user may have to the first portion. In any event, for reasons to be discussed, the unique public IP address assigned by the MNO is stored in the first portion, and the processor **52** prohibits access thereto. However, other types of information, such as sensitive user information, such as user name, credit card, etc. may also be stored in the first portion and the processor **52** may grant the user limited access to those type of information.

After the removable card **10** of the present invention is distributed to users, and the user has inserted the card **10** into the device **100** of the present invention, the user can then use the device **100** to operate on the cellular network **110**, as it was done in the prior art. Similar to the prior art, the card **10** may also have information related to the usage of the device **100**, such as telephone number, access code, number of minutes, calling plan etc on the cellular network **110** stored in the first portion (user restricted) of the memory portion of the card **10**. Clearly the storage of this type of information in the user restricted is appropriate, so that the user cannot have unlimited access. In this manner, the removable card **10** functions no differently than the SIM card of the prior art when used with the cellular network **110**.

The inventive features of the present invention can be seen when the user attempts to use the device **100** to access the Internet **150**. There are at least two possible modes (first mode or second mode) to access the Internet **150**. The programming code stored in the non-volatile memory **14** can cause the processor **52** to access the Internet **150** in either the first mode or the second mode of operation.

In the first mode, the Internet **150** can be accessed by the removable card **10** through the device **100** through the cellular network **110**. In that event the device **100** is connected to the Internet **150** through the access servers connected to the cellular network **110**, near the tower **120**. When initiated, the access servers (similar to an Internet Service Provider (ISP)) may assign a dynamic public IP address to the device **100** during the session connecting the device **100** to the Internet **150**. Such dynamic assignment of public IP addresses when the device **100** is connected to the Internet **150** is well known in the art and is in accordance with the DHCP protocol. Alternatively, as discussed previously, the public IP address may be pre-assigned and stored in the removable card **10**. The browser and media player **112** of the device **100** is then used to browse or surf the Internet **150**. Contents from the Internet **150** can then be downloaded and saved in the removable card **10**, in either the user restricted memory portion or the user accessible portion of the card **10**.

For secure communication with the Internet, the user restricted portion of the memory portion of the card **10** may store a secret key. The RSA/AES/DES engine **60** of the host controller **12** can use that secret key to encrypt and/or decrypt communication to and from the Internet **150**. The secret key can be provided by the MNO when it initially distributes the removable card **10** or it can be downloaded from the MNO server **200** which is connected to the Internet **150**, when the device is connected to the Internet **150**.

There are two ways by which the RSA/AES/DES engine **60** of the host controller **12** can securely use the secret key stored in the user restricted memory portion of the card **10**, to encrypt and/or decrypt communication to and from the Internet **150**. First, assume that the host controller **12**, and the memory controller **14** and NAND memory **20** and PSRAM **22** are all integrated in a single integrated circuit. Then the secret key can be stored in the NAND memory **20**, retrieved by the memory controller **14** and provided to the RSA/AES/DES engine **60** of the host controller **12** to encrypt messages to the Internet **150**. Conversely, messages or information from the Internet **150** received by the device **100** may be decrypted by the RSA/AES/DES engine **60** of the host controller **12** using the secret key, and then the decrypted information further processed, stored, displayed or acted upon.

Alternatively, because the host controller **12**, the memory controller **14** and the NAND memory **20** may be large semiconductor dies, it may be impractical and/or uneconomical to integrated all of them into a single integrated circuit die. Thus, the host controller **12**, the memory controller **14** and the NAND memory **20** might all be packaged into a SIP (System-In-Package) module, with the memory controller **14** and the NAND memory **20** integrated into a single semiconductor die, and with the host controller **12** in another single semiconductor die. In that event, if the secret key is stored in the NAND memory die **20**, then that secret key may be vulnerable to discovery by an unscrupulous third party who opens the removable card **10** and probes the bus **16**. To overcome this potential vulnerability, the host controller **12** after boot up will execute a program to generate a random key pair. This program may be a random number generator. Thus, the key pair that is generated is effective only for the duration of that session (i.e. valid only for as long as power is supplied). The key pair, which is a technology well known, consists of a public key and a private key. The public key portion is supplied to the memory controller **14** across the bus **16**. The memory controller **14** encrypts the secret key from the NAND memory **20** using the public key, and returns that encrypted result to the host controller **12** across the bus **16**. The host controller **12** then decrypts that result using the private key portion of the key pair and extracts the secret key that was originally stored in the NAND memory **20**. The host controller **12** then uses the secret key to encrypt data to the Internet **150**. The same secret key is of course also used to decrypt the data received from the Internet **150**. The encryption of the secret key using the public key by the memory controller is done only once during boot up. After the secret key is encrypted and is supplied to the host controller **12**, it is decrypted and the secret key is then stored in the SRAM **64**. Thereafter, it is used during access to/from the Internet **150**. Of course, once the session is over, and the power removed from the device **100** and the removable card **10**, the secret key in the SRAM **64** is lost, and the procedure of generating a key pair upon boot up must be done again.

The information retrieved from the Internet **150**, via the wireless network **110**, may be saved in the user restricted portion of the removable card **10** which is associated with an assigned private IP address. The private IP address can be first assigned by the MNO and stored in the removable card **10** before distribution. Alternatively, the private address may be assigned by the access server connected to the cellular network **120**. Finally, the private address may simply be the public IP address dynamically assigned by the access severs and then translated by the NAT circuit **106** into a private IP address. After the information from the Internet **150** is stored in the removable card **10**, it can be retrieved by the browser and media player **112**, and displayed on the display **108** of the device **100**, using the private IP address. This is similar to the operation of an intranet. Thus, the removable card **10** serves to function as a local (private) server in providing the data stored in its memory to the browser and media player **112**.

The use of a "private" IP address when the browser **112** is accessing in a local mode is advantageous because it is more economical than having two public IP address assigned to the device **100**: one IP address for the phone portion of the device **100** when surfing or browsing the Internet **150** and another public IP address for the removable card **10**, when viewing the contents thereof. Since the content stored in the removable card **10** is for the user using the device **100**, there is no need for the removable card **10** to have a public IP address. Furthermore, the time when the user is viewing the contents stored in the removable card **10**, the device **100** may not be connected to the Internet **150**.

In a second mode, the device **100** can access the Internet **150** other than through the cellular network **110**. One way is through a network portal device **170** such as a terminal connected to a PC (for example through a USB port). Another way is through a wireless link, such as Wi-Fi which connects wirelessly to a receiving device (not shown) that is connected to the Internet **150**. In either way, the device **100** has a docking switch **160**. Referring to FIG. **5**, there is shown schematically a diagram of this mode of communication (along with the first mode) Normally, in the first mode, the removable card **10** is connected to the USB interface **114** through the docking switch **160**. However, when the device **100** is connected to the PC **170** or through the NFC **24**, the docking switch **160** is changed causing the removable card **10** to disconnect from the USB interface **114**. Thus, for example, when a USB cable is connected to the docking switch **160**, the removable card **10** disconnects from the USB interface **114** and connects directly to the PC **170** along its USB port. The docking switch **160** then breaks the connection between the removable card **10** and the rest of the device **100** including the transceiver **104**. Because the removable card **10** contains the cellular network **110** access information, if the device **100** was accessing the

Internet wirelessly through the cellular network **110**, then the device **100** would cease to transmit/receive wirelessly to/from the cellular network **110**. Similar to the first mode of operation, when the device **100** is connected to the Internet **150** through the docking switch **160**, to the PC gateway **170**, it is initially assigned a public IP address, by the Internet Service Provider (ISP) for connection to the Internet **150**. Again, this is a dynamically assigned public IP address for use during the session that the device **100** is connected to the Internet **150**.

Finally, because the removable card **10** stores a public IP address assigned by the MNO, in the user restricted portion of the memory, that public IP address directs the device **100** to the MNO server **200**. During the time period when the device **100** is connected to the Internet **150** through the PC portal **170**, and when the user is not browsing or surfing the Internet **150**, (as in e.g. when the device **100** is in the docking station connected to the docking switch **160** for charging the battery for the device **100**) the device **100** can go the MNO server **200** using the public IP address stored in the removable card **10**. The MNO server **200** can then cause content, such as movies, or programming code (updates for the device **100**) to be downloaded and stored in the user restricted portion of the removable card **10** of the device **100**. The benefit of this mode is that a large amount of content can be downloaded when the device **100** is not connected to the cellular network **110**, and when the user is not actively surfing or browsing the Internet **150**. The downloaded movies or other material can be subsequently activated by an authorization code and/or payment code. Since the movies or other content were downloaded from the MNO server **200**, the user can be sure of the trustworthiness of the content (i.e. free from virus etc.). In addition, since the owner of the content knows that the content is downloaded in a secure manner and stored in a user restricted portion, they can be assured that illicit copies will not be made. In this manner, this becomes a trustworthy procedure for all parties. Finally, by also permitting programming code to be distributed in this manner, an efficient and convenient mode is provided to assure the update of the devices **100**.

Furthermore, each removable card **10** may also be assigned a unique IP address by the MNO operator. This offers another unique feature of the present invention. When the device **100** with the removable card **10** connected thereto is connected to the Internet **150**, and with the removable card **10** having a unique IP address, the MNO server **200** which is also connected to the Internet **150** can download information for all removable cards **10** or just certain removable cards **10** or even only a specific removable card **10**. The information downloaded to one or more removable cards **10** may be stored in the user restricted memory portion of the card **10**. Examples of information that can be stored in the user restricted portion may include: administrative information such as change in calling plan, increase in minutes etc. Further, the "information" may be data or it may be programming code (including Java applets) for execution by the host controller **12**. Thus, for example, the "information" downloaded from the MNO server **200** may be a program causing the host controller **12** to execute the code causing the device **100** to access the cellular network **110** to access the Internet **150** periodically or to access specified location on the Internet **150** (such as the IP address of the MNO server **200**) or in some specified manner to retrieve updates, downloads, etc.

Although the foregoing has described the invention for use in a SIM module in a cell phone, it should be clear that the present invention may be used in any removable card that stores secured information.

What is claimed is:

1. A secure removable card having electrical connections for communication therewith, comprising:

a first integrated circuit die, said first die including a processor;

a second integrated circuit die, said second die including a non-volatile memory for storing a secret key, and a controller for controlling the operation of the non-volatile memory;

a bus connecting the first die with the second die;

wherein the processor for generating a key pair, having a public key portion and a private key portion upon power up, with said key pair generated not based upon stored data, and for transferring the public key portion across the bus to the second die;

wherein the controller for receiving the public key and for encrypting the secret key with the public key to generate a first encrypted key, and for transferring the first encrypted key across the bus to the first die; and

wherein the processor for receiving the first encrypted key and for decrypting the first encrypted key to recover the secret key; and for encrypting data with said secret key for communicating along the electrical connections external to the card.

2. The card of claim **1** wherein said first die further includes a volatile memory embedded with said processor;

wherein said volatile memory for storing the secret key.

3. The card of claim **2** wherein said first die further comprising a random number generator, wherein the random number generator generate the public key portion and the private key portion.

4. The card of claim **1** wherein said processor decrypts the first encrypted key using the private key portion.

5. A method of securely communicating with a removable card, said card having electrical connections thereto, and having a first semiconductor die, a second semiconductor die with an electrical bus connecting the first die with the second die, packaged together, said first die having a processor, said second die having a non-volatile memory for storing a secret key, and a controller for controlling the operation of the non-volatile memory, said method comprising:

generating a key pair, upon power up of the processor, having a public key and a private key by the processor, wherein said key pair generated is not based upon stored data;

transferring the public key to the second die via the electrical bus;

encrypting the secret key using the public key by the controller to produce an encrypted key;

transferring the encrypted key to the first die via the electrical bus;

decrypting the encrypted key to extract the secret key by the processor; and

using the secret key to encrypt data to communicate on the electrical connections external to the card.

6. The method of claim **5** wherein said key pair is generated by a random number generator.

7. The method of claim **6** wherein said secret key is stored in a volatile memory embedded in the processor.

8. The method of claim **5** wherein said key pair is generated upon power up.

9. The method of claim **5** wherein said encrypted key is decrypted by using the secret key.

* * * * *

APPENDIX
TAB B

US008200281B2

(12) **United States Patent**
Yeh

(10) **Patent No.: US 8,200,281 B2**
(45) **Date of Patent: Jun. 12, 2012**

(54) **SECURE REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE**

(75) Inventor: **Bing Yeh**, Los Altos Hills, CA (US)

(73) Assignee: **Greenliant LLC**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 442 days.

(21) Appl. No.: **12/502,897**

(22) Filed: **Jul. 14, 2009**

(65) **Prior Publication Data**

US 2011/0014948 A1 Jan. 20, 2011

(51) **Int. Cl.**

H04M 1/00	(2006.01)
H04B 1/38	(2006.01)
H04M 9/00	(2006.01)
H04M 1/66	(2006.01)
H04M 1/68	(2006.01)
H04M 3/16	(2006.01)

(52) **U.S. Cl.** **455/558**; 379/433.09; 455/410; 455/411

(58) **Field of Classification Search** 455/558, 455/410–411; 379/433.09
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2007/0074273	A1 *	3/2007	Linden	726/3
2008/0288700	A1 *	11/2008	Holtzman et al.	710/301

OTHER PUBLICATIONS

PCT Search Report and Written Opinion mailed on Sep. 30, 2010 corresponding to the related PCT Patent Application No. US10/45394.

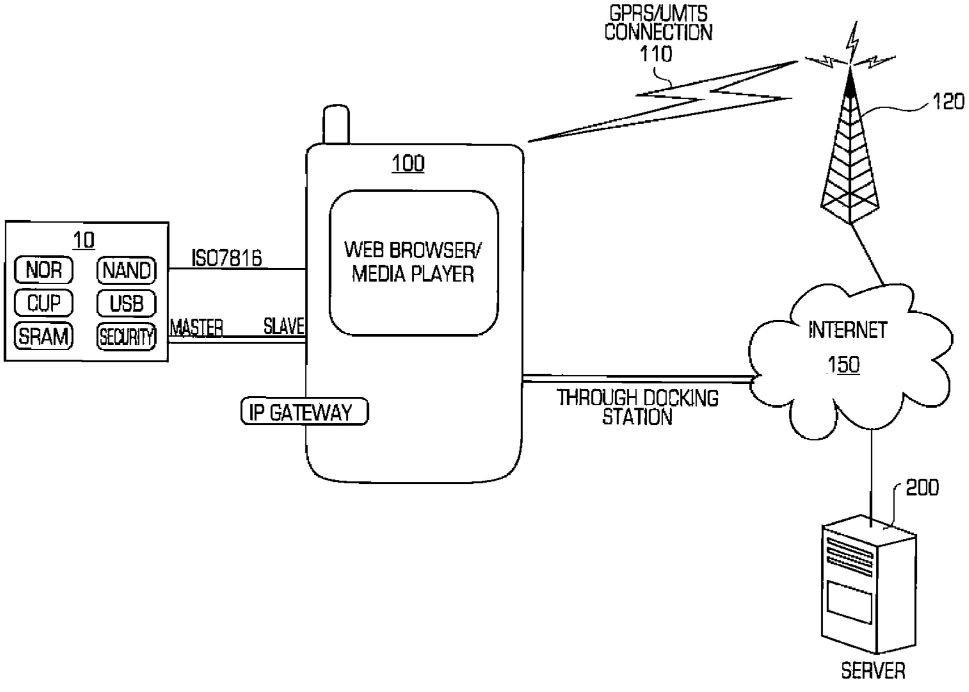
* cited by examiner

Primary Examiner — Vladimir Magloire
Assistant Examiner — Munsoon Choo
(74) *Attorney, Agent, or Firm* — DLA Piper LLP (US)

(57) **ABSTRACT**

A removable card for use with a mobile wireless communication device has a processor and a non-volatile memory, connected to the processor. The removable card has electrical connections for connecting to a mobile wireless communicating device for use by a user to access a common carrier network to access a network of interconnected computer networks ("Internet"). The card comprises a processor and a non-volatile memory connected to the processor. The non-volatile memory has two portions: a first portion and a second portion. The first portion is accessible by the provider of the common carrier network with the processor restricting access thereto by the user. The second portion is accessible by the provider of the common carrier network and with the processor granting access thereto to the user for storing user data therein. Finally, the removable card has logic circuit for encoding the user data to produce encrypted user data, for storing in the second portion.

9 Claims, 5 Drawing Sheets



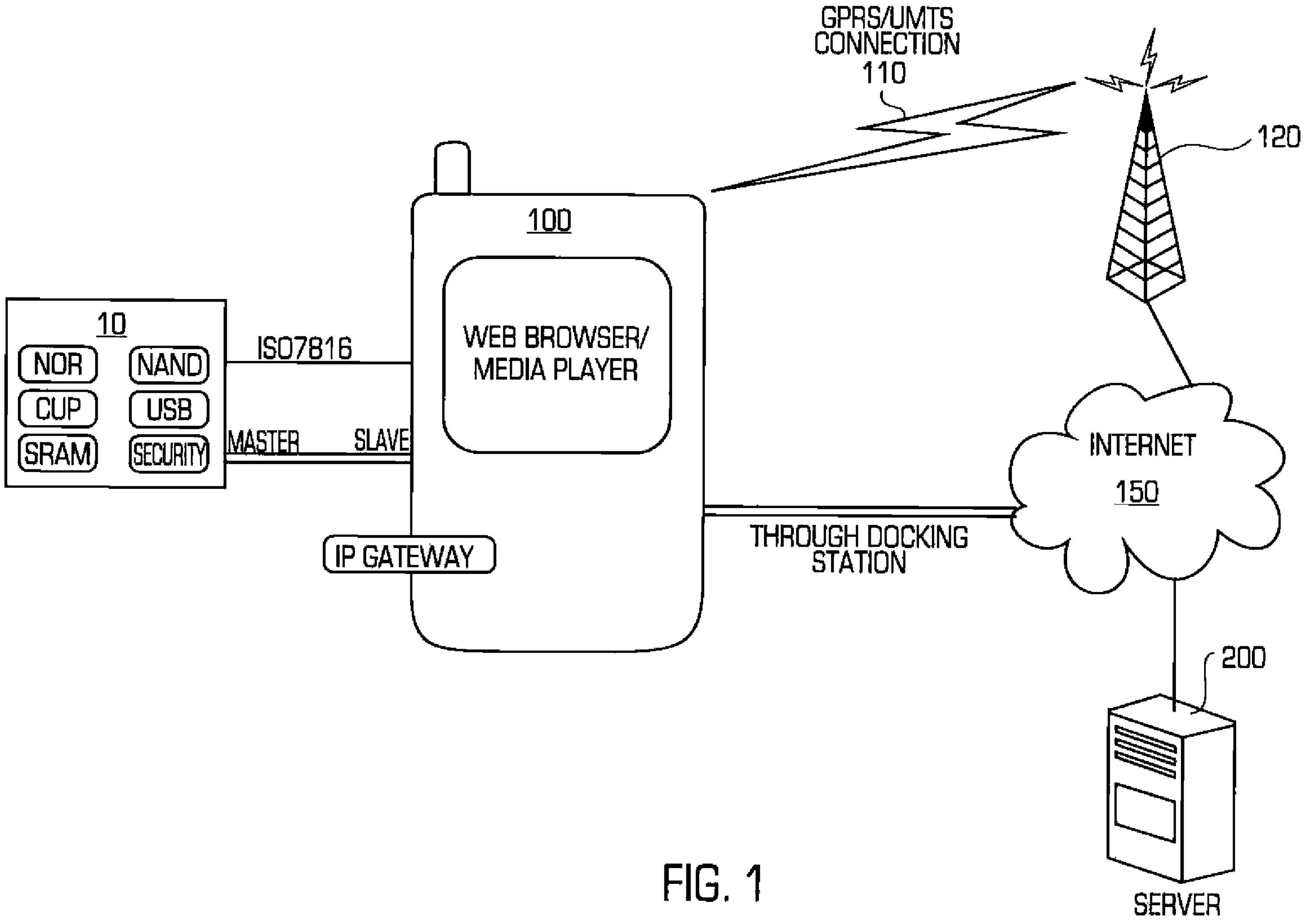

GPRS/UMTS CONNECTION
110
120
100
10
NOR
NAND
CUP
USB
SRAM
SECURITY
ISO7816
MASTER
SLAVE
WEB BROWSER/ MEDIA PLAYER
IP GATEWAY
THROUGH DOCKING STATION
INTERNET
150
200
SERVER

FIG. 1

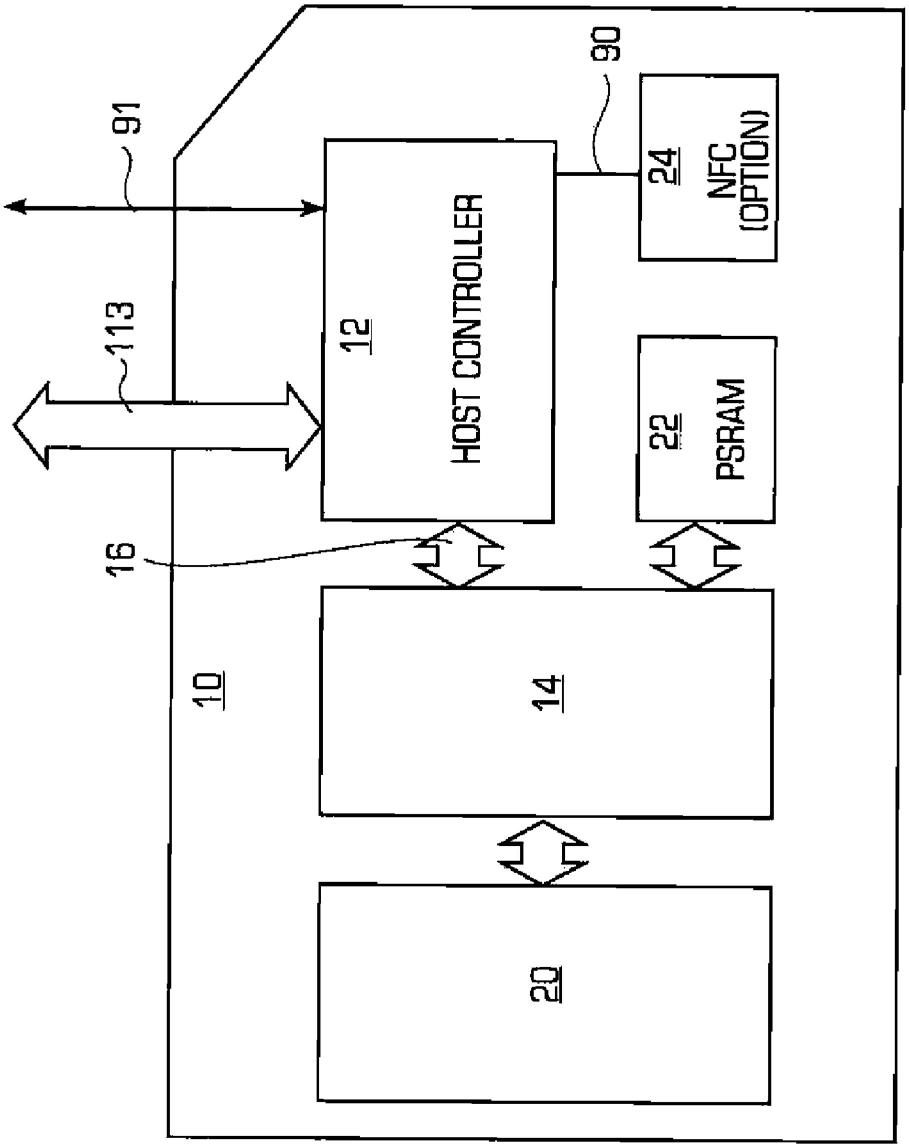

91
90
113
12
HOST CONTROLLER
24
NFC
(OPTION)
22
PSRAM
16
10
14
20

FIG. 3

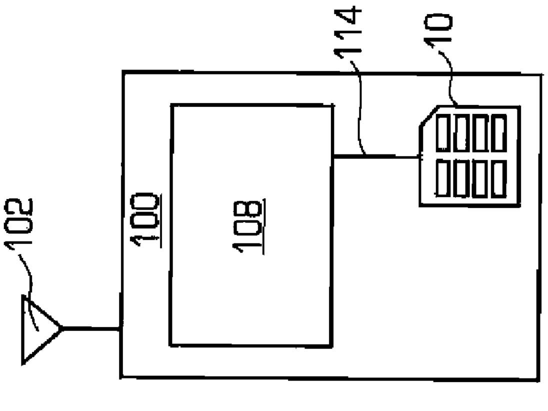

114
10
102
100
108

FIG. 2

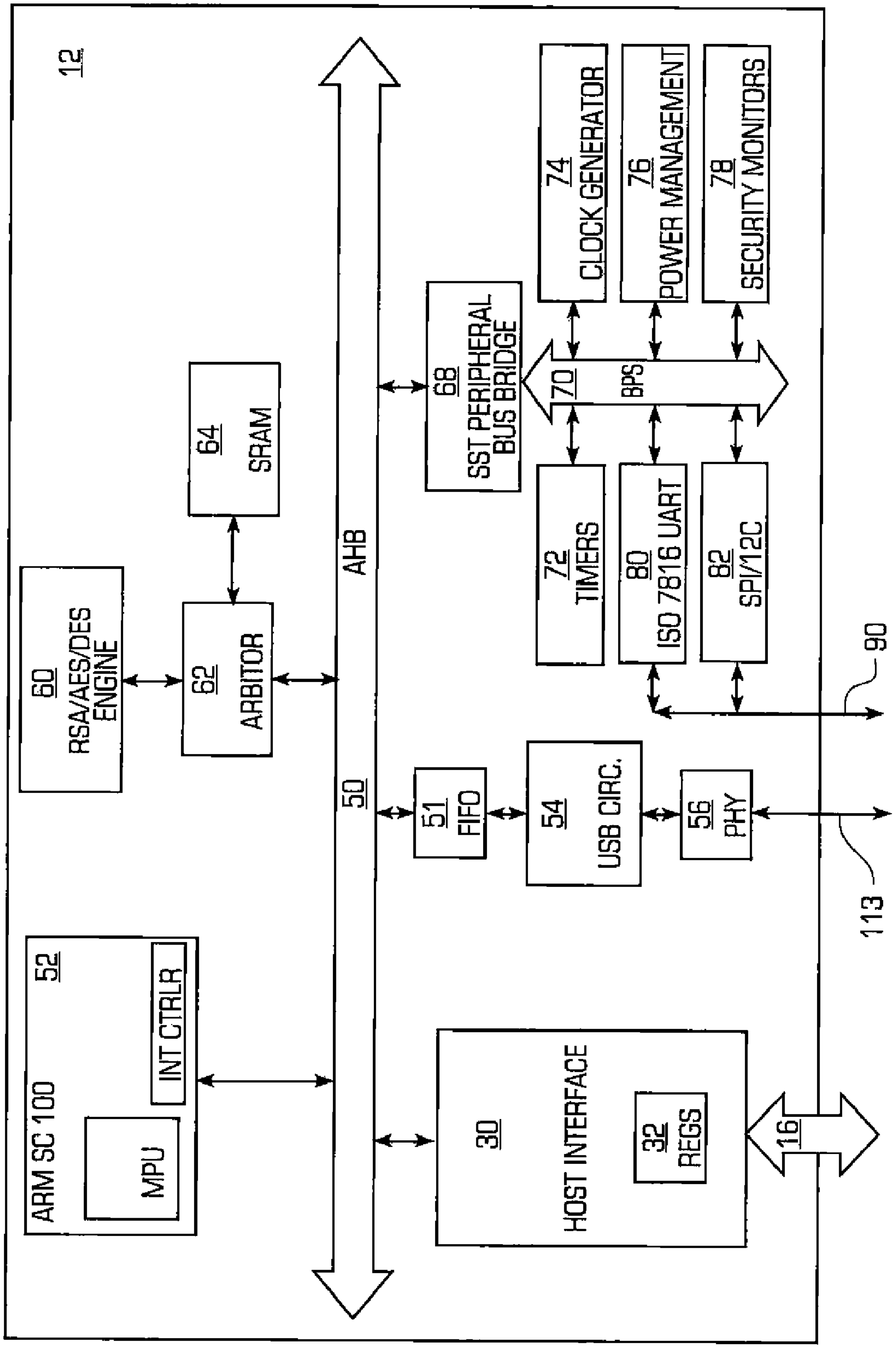

12
ARM SC 100
52
MPU
INT CTRLR
60
RSA/AES/DES ENGINE
62
ARBITOR
64
SRAM
AHB
50
68
SST PERIPHERAL BUS BRIDGE
70
BPS
74
CLOCK GENERATOR
76
POWER MANAGEMENT
78
SECURITY MONITORS
72
TIMERS
80
ISO 7816 UART
82
SPI/12C
90
51
FIFO
54
USB CIRC.
56
PHY
113
30
HOST INTERFACE
32
REGS
16

FIG. 4

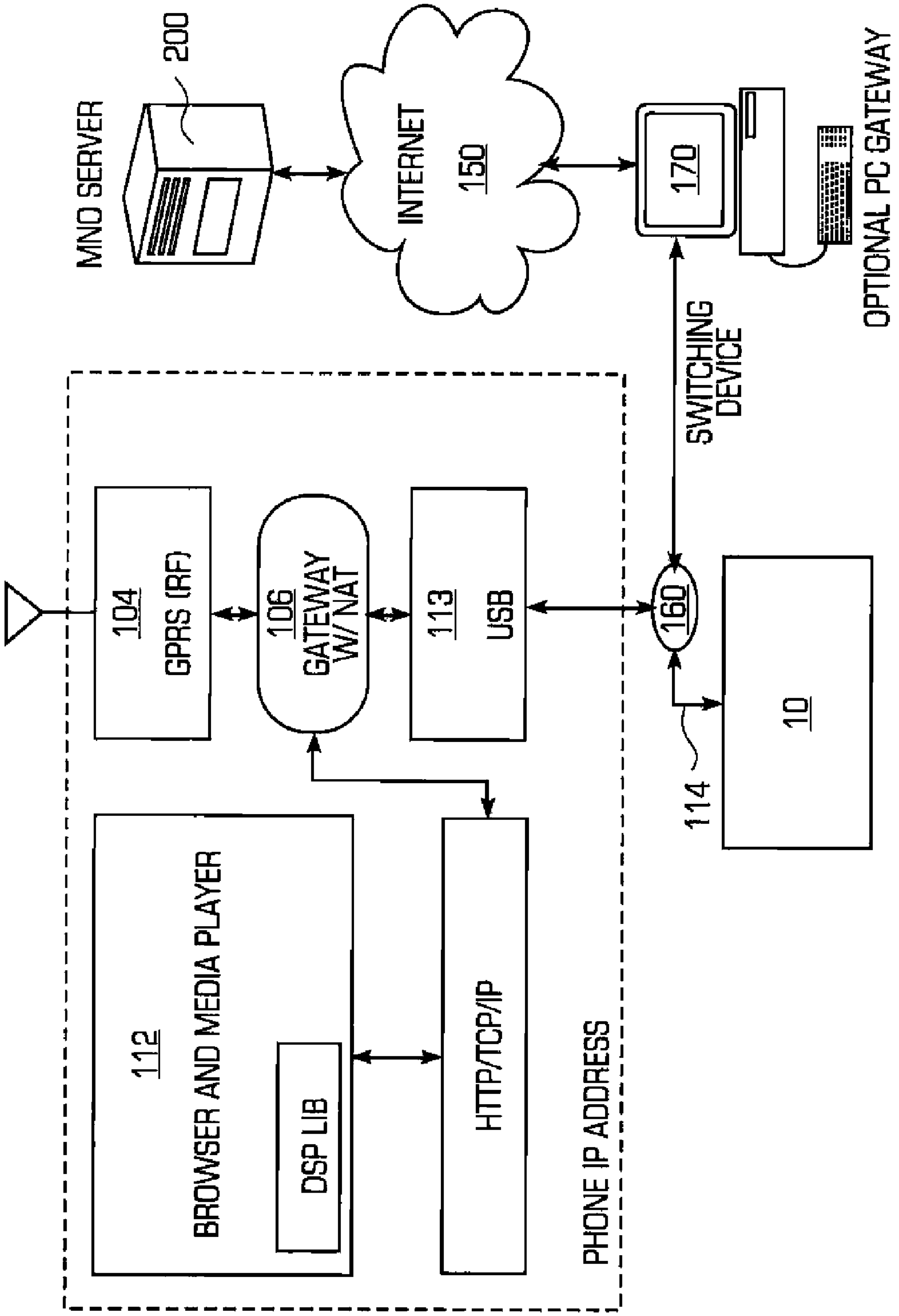

MND SERVER
200
INTERNET
150
170
OPTIONAL PC GATEWAY
SWITCHING DEVICE
104
GPRS (RF)
106
GATEWAY W/ NAT
113
USB
160
10
114
112
BROWSER AND MEDIA PLAYER
DSP LIB
HTTP/TCP/IP
PHONE IP ADDRESS

FIG. 5

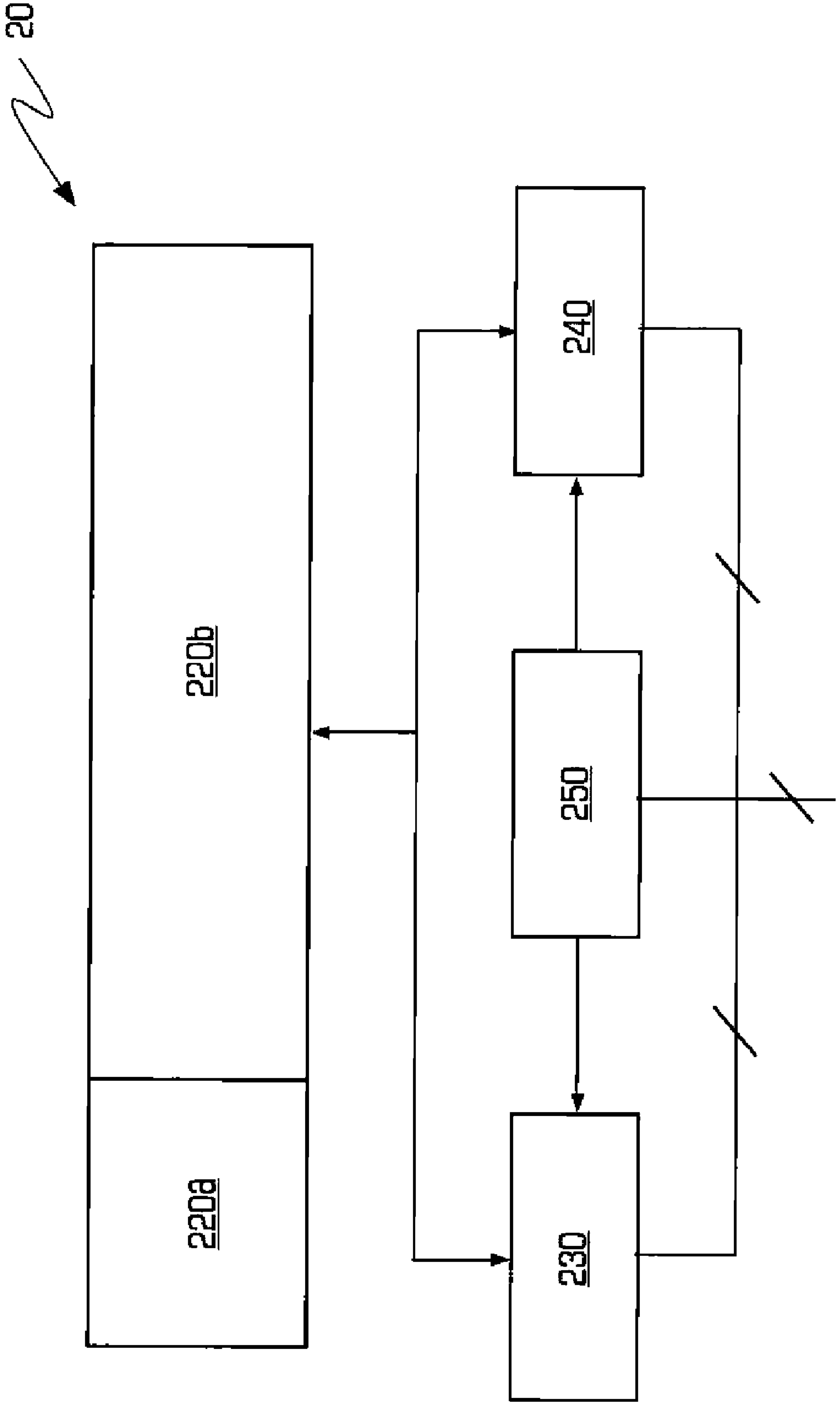


FIG. 6

SECURE REMOVABLE CARD AND A MOBILE WIRELESS COMMUNICATION DEVICE

TECHNICAL FIELD

The present invention relates to a secured removable card having a processor and a non-volatile memory and is suitable for use with a mobile wireless communication device, for connecting to a network of interconnected computer networks ("Internet") in which the non-volatile memory stores program code configured to be executed by the processor and user data. The removable card has a processor and a memory with two portions, with the processor restricting access to the first portion by the user, and granting user access to the second portion to store user data. However, because the network carrier provider has access to both portions and can store the user data in the second portion on the Internet as backup, the user data in the second portion must be rendered secure even from the network carrier.

BACKGROUND OF THE INVENTION

Mobile wireless communication devices, such as cell phones are well known in the art. Typically, a cell phone has a removable card (called "SIM card") which consists of a processor with RAM, ROM or EEPROM or Flash memory, I/O pads, and security monitoring circuit all mounted on a removable card. The non-volatile memory in the SIM card is to store information required to access the mobile operator's network. Thus, the card may store information such as telephone number, access code, number of minutes, calling plan etc.

A network of interconnected computer networks ("Internet") is also well known in the art. The Internet can be accessed by computers having a direct connection (wired or wireless), or through a common carrier wireless network.

With the increase in speed in mobile networks, such as the 3G network, users of mobile wireless devices desire to access the Internet via their mobile wireless communication devices. Even though the speed of the mobile network is increasing, the cost of using that network may also increases with greater use of the common carrier network, especially when accessing the Internet.

Hence, it is desirable to provide a mechanism whereby the user's experience to access the Internet through the mobile network is not diminished, but at the same time, providing means to reduce the cost of accessing the Internet through the mobile network. Further, as the cost of storage capacity continues to decrease, increasingly, the user will store valuable information including person and private information in such portable devices. Because the mobile device can access the Internet, the provider of the common carrier service may offer the service of backing up that data on the Internet. Thus, it is desired to secure the data stored in such portable mobile device. Further, even if the common carrier provider does not offer Internet data back up service, the user may still desire to secure the data, since the portable mobile device can easily be lost or stolen.

Thus, is desired that the data supplied by the user be securely stored in such a mobile device.

SUMMARY OF THE INVENTION

Accordingly, in the present invention, a removable card has electrical connections for connecting to a mobile wireless communicating device for use by a user to access a common carrier network to access a network of interconnected computer networks ("Internet"). The card comprises a processor and a non-volatile memory connected to the processor. The non-volatile memory has two portions: a first portion and a second portion. The first portion is accessible by the provider of the common carrier network with the processor restricting access thereto by the user. The second portion is accessible by the provider of the common carrier network and with the processor granting access thereto to the user for storing user data therein. Finally, the removable card has logic circuit for encoding the user data to produce encrypted user data, for storing in the second portion.

The present invention also relates to a mobile wireless communication device for use by a user to access a common carrier network to access a network of interconnected computer networks ("Internet"). The device comprises a transceiver for communication wirelessly via a wireless common carrier network. The device further has a first processor for controlling communication of the device to connect to the common carrier network. The device further has a second processor and a non-volatile memory connected to the second processor. The non-volatile memory has two portions: a first portion and a second portion. The first portion is accessible by the provider of the common carrier network with the second processor restricting access thereto by the user. The second portion is accessible by the provider of the common carrier network and with the second processor granting access thereto to the user for storing user data therein. Finally the device has a logic circuit for encoding the user data to produce encrypted user data for storing in the second portion.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a diagram of the removable card of the present invention connected to a mobile wireless communication device of the present invention for connection to a mobile network, as well as to the Internet.

FIG. **2** is a schematic diagram of the removable card of the present invention connected to the mobile wireless communication device of the present invention.

FIG. **3** is a block level diagram circuit diagram of the removable card of the present invention.

FIG. **4** is a detailed circuit diagram of the processor portion of the removable card of the present invention.

FIG. **5** is a diagram of the two modes of communication of the mobile wireless communication device with the removable card of the present invention with the Internet, wherein in the first mode, the removable card communicates through the wireless communication device wirelessly with the mobile network for access to the Internet, and wherein in a second mode the removable card is connected to a network portal device for connection to the Internet.

FIG. **6** is a block level diagram of the removable card of the present invention with its security feature.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to FIG. **1** there is a shown a graphic illustration of a mobile wireless communication device **100**, e.g. a cell phone **100** for use in a publicly accessible (common carrier) wireless communication network, such as a cellular network **110**, which includes cellular access towers **120**. The cellular network **110**, through access servers (not shown) located on or near the cell phone towers **120** can connect to a network of interconnected computer networks **150**, also known as the Internet **150**. Thus, the cell phone **100** can communicate wirelessly with other cell phones **100** on the cell phone network **110**. In addition, the cell phone **100** can communicate wirelessly with the Internet **150** through the cell phone network **110** which has the access servers connected to the Internet **150**. Further, as will be shown hereinbelow, the removable card **10** portion of the cell phone **100** can also be connected directly to the Internet **150** through a network portal device, such as docking station **160**, which is connected to a personal computer, which connects to the Internet **150**.

The cell phone **100** of the present invention has a removable card **10**, much like the removable SIM card of the prior art. However, as will be seen, the features of the removable card **10** of the present invention are vastly different and improved over the removable SIM card of the prior art.

Referring to FIG. **2**, there is shown a schematic diagram of the removable card **10** of the present invention connected to the mobile wireless communication device **100** of the present invention. Because the device **100** is designed to operate wirelessly across the cellular network **110**, the device **100** comprises an antenna **102**. A transceiver **104** is connected to the antenna **102**. The transceiver **104** transmits and receives modulated signals to and from the cellular network **110**. Such components are well known in the art. The received signals may be demodulated and then converted into digital signals and provided to a gateway **106**. The gateway **106** may also have an NAT (Network Address Translation) circuit. An NAT circuit **106** translates or maps a private IP address to one or more ports of a public IP address. As will be discussed hereinafter, the device **100** (through the removable card **10**), may be assigned a public address (through the well known DHCP protocol) when the device is connected to the Internet **150**, and may have a private address when operating as a local server such that the device **100** is not connected to the Internet **150**. Digital signals to be transmitted are modulated and converted by the transceiver **104** into appropriate electromagnetic frequency signals for transmission by the antenna **102**. Because the device **100** can access the Internet **150**, a browser and media player **112** is also provided. The browser and media player **112** interfaces in the well known TCP/IP protocol as well as the HTTP protocol with the gateway **106** to provide and to receive digital signals received by the device **100** from the Internet **150**, which may be displayed on a display **108**. Associated with the browser and media player **112** is a processor (not shown) which also controls the transceiver **104** and other well known hardware circuits of the device **100** to communicate with the network **110**.

The removable card **10** of the present invention is connected to the device **100** through a well known USB interface **114** through the docking station **160**. The USB interface **114** connects to the Gateway **106**. Thus, digital signals from the removable card **10** are provided to and from the device **100** through the docking station **160**, through the USB interface **114**, through the gateway **106** and through the transceiver **104** to the antenna **102**.

The removable card **10** of the present invention is shown in greater detail in FIG. **3**. in particular, the card **10** comprises a host controller **12** which interfaces with the USB interface **114** through a USB bus **113**. In addition, the host controller **12** is connected to a memory controller **14**, through a bus **16**. The memory controller **14** controls a NAND memory **20** and a PSRAM **22**. The operation of the memory controller **14** in controlling the NAND memory **20** and the PSRAM **22** is fully described in U.S. patent application Ser. No. 11/637,420, published on Jun. 28, 2007 under publication 2007-0147115, and assigned to the present assignee, which disclosure is incorporated by reference herein in its entirety. The host controller **12** may also be optionally connected to a Near Field Communicator (NFC) **24**. An NFC **24** is a close range RF circuit that permits wireless communication in close proximity. Thus, the device **100** with the NFC **24** may act as an "electronic wallet" for financial transactions or for identification purpose, or as another access to the Internet **150**. Of course, the device **100** can also be connected wirelessly with the Internet **150** via other forms of wireless networks, such as a Wi-Fi network.

Referring to FIG. **4**, there is shown a detailed schematic block diagram of the host controller **12**. The host controller **12** comprises a high speed bus **50**, to which a host interface **30**, for connecting to the memory controller **14** is attached. The host interface **30** also comprises registers **32** for temporarily holding data that is supplied to and from the memory controller **14**. The host controller **12** also comprises a FIFO (First-In First Out) circuit **51** which is connected to the high speed bus **50**. The FIFO **51** is also connected to a USB controller circuit **54**, which is connected to a PHY circuit **56** (which is the standard physical layer interface for a USB port. The circuit **56** includes pads, voltage level shifters and clock recovery circuits.) for connection to the USB bus **113**. A secure processor, such as an ARM SC-100 processor **52** is also connected to the high speed bus **50**.

The host controller **12** also comprises a RSA/AES/DES engine **60**, which is a secure co-processor to the ARM SC-100 processor **52**. The engine **60** is connected to the high speed bus **50** through an arbitration circuit **62**. Since both the engine **60** and the processor **52** can request memory or other resources of the high speed bus **50** at the same time, the arbitration circuit **62** arbitrates simultaneous requests for access to the bus **50**. The engine **60** also has access to a dedicated high speed cache RAM, such as an SRAM **64**. Finally, a bridge circuit **68** is also connected to the high speed bus **50**. The bridge circuit **68** is also connected to a slower bus **70**, to which a timer **72** is connected, a clock generator **74** is connected, a power management circuit **76** is connected, a security monitoring circuit **78** is connected, a UART **80** is connected, and a SPI circuit **82** (Serial Peripheral Interface—a well known bus) is connected. The UART **80** and the SPI **82** are also connected to a bus **90**, which is connected to the NFC **24**. The controller **12** is also connected to a bus **91** which is a ISO7816 serial interface bus. It is a byte oriented Universal Asynchronous Receiver/Transmitter (UART) interface commonly found in prior art cell phones between the phone and the SIM card. This type of interface (using UART) is being replaced by the USB interface. Thus, the presence of the bus **91** is for backward compatibility only.

Operation of the Mobile Wireless Communication Device

There are many modes of operation of the mobile wireless communication device **100** of the present invention. Initially, it should be noted that the mobile network operator (MNO), the operator of the cellular network **110**, distributes each of the removable cards **10**, and also has a server **200** connected to the Internet **150**. Each of the removable cards **10** of the present invention distributed by the MNO is assigned a unique public IP address by the MNO which is stored in the non-volatile memory portion of the removable card **10**. The unique public IP address directs the device **100** to the MNO server **200**. As disclosed in U.S. patent application Ser. No. 11/637,420, published on Jun. 28, 2007 under publication 2007-0147115, non-volatile memory is present in the NAND memory **20** as well as NOR memory being embedded in the controller **14**. In either event, the MNO assigns and pre-stores a unique public IP address in the non-volatile memory portion of the removable card **10**. The non-volatile memory may be divided into two portions, with the partition between the first portion **220***a* and the second portion **220***b* being alterable.

The partitioning of the first portion/second portion can be done by the MNO provider of the removable card **10**. The first portion **220***a* can be accessed by the processor which controls the transceiver **104** and browser and media player **112**, and the other hardware circuits that control the communication of the device **100**. The second portion **220***b* can be accessed by the processor **52**, in the removable card **10**, which is accessible by the user. In addition, the processor **52** controls the degree of access (which includes the type of information) that a user may have to the first portion **220***a*. In any event, for reasons to be discussed, the unique public IP address assigned by the MNO is stored in the first portion **220***a*, and the processor **52** prohibits access thereto. However, other types of information, such as sensitive user information, such as user name, credit card, etc. may also be stored in the first portion **220***a* and the processor **52** may grant the user limited access to those type of information.

After the removable card **10** of the present invention is distributed to users, and the user has inserted the card **10** into the device **100** of the present invention, the user can then use the device **100** to operate on the cellular network **110**, as it was done in the prior art. Similar to the prior art, the card **10** may also have information related to the usage of the device **100**, such as telephone number, access code, number of minutes, calling plan etc on the cellular network **110** stored in the first portion **220***a* (user restricted) of the memory portion of the card **10**. Clearly the storage of this type of information in the user restricted is appropriate, so that the user cannot have unlimited access. In this manner, the removable card **10** functions no differently than the SIM card of the prior art when used with the cellular network **110**.

The inventive features of the present invention can be seen when the user attempts to use the device **100** to access the Internet **150**. There are at least two possible modes (first mode or second mode) to access the Internet **150**. The programming code stored in the non-volatile memory **14** can cause the processor **52** to access the Internet **150** in either the first mode or the second mode of operation.

In the first mode, the Internet **150** can be accessed by the removable card **10** through the device **100** through the cellular network **110**. In that event the device **100** is connected to the Internet **150** through the access servers connected to the cellular network **110**, near the tower **120**. When initiated, the access servers (similar to an Internet Service Provider (ISP)) may assign a dynamic public IP address to the device **100** during the session connecting the device **100** to the Internet **150**. Such dynamic assignment of public IP addresses when the device **100** is connected to the Internet **150** is well known in the art and is in accordance with the DHCP protocol. Alternatively, as discussed previously, the public IP address may be pre-assigned and stored in the removable card **10**. The browser and media player **112** of the device **100** is then used to browse or surf the Internet **150**. Contents from the Internet **150** can then be downloaded and saved in the removable card **10**, in either the user restricted memory portion or the user accessible portion of the card **10**.

For secure communication with the Internet, the user restricted portion of the memory portion of the card **10** may store a secret key. The RSA/AES/DES engine **60** of the host controller **12** can use that secret key to encrypt and/or decrypt communication to and from the Internet **150**. The secret key can be provided by the MNO when it initially distributes the removable card **10** or it can be downloaded from the MNO server **200** which is connected to the Internet **150**, when the device is connected to the Internet **150**.

The information retrieved from the Internet **150**, via the wireless network **110**, may be saved in the user restricted portion of the removable card **10** which is associated with an assigned private IP address. The private IP address can be first assigned by the MNO and stored in the removable card **10** before distribution. Alternatively, the private address may be assigned by the access server connected to the cellular network **120**. Finally, the private address may simply be the public IP address dynamically assigned by the access severs and then translated by the NAT circuit **106** into a private IP address. After the information from the Internet **150** is stored in the removable card **10**, it can be retrieved by the browser and media player **112**, and displayed on the display **108** of the device **100**, using the private IP address. This is similar to the operation of an intranet. Thus, the removable card **10** serves to function as a local (private) server in providing the data stored in its memory to the browser and media player **112**.

The use of a "private" IP address when the browser **112** is accessing in a local mode is advantageous because it is more economical than having two public IP address assigned to the device **100**: one IP address for the phone portion of the device **100** when surfing or browsing the Internet **150** and another public IP address for the removable card **10**, when viewing the contents thereof. Since the content stored in the removable card **10** is for the user using the device **100**, there is no need for the removable card **10** to have a public IP address. Furthermore, the time when the user is viewing the contents stored in the removable card **10**, the device **100** may not be connected to the Internet **150**.

In a second mode, the device **100** can access the Internet **150** other than through the cellular network **110**. One way is through a network portal device **170** such as a terminal connected to a PC (for example through a USB port). Another way is through a wireless link, such as Wi-Fi which connects wirelessly to a receiving device (not shown) that is connected to the Internet **150**. In either way, the device **100** has a docking switch **160**. Referring to FIG. **5**, there is shown schematically a diagram of this mode of communication (along with the first mode) Normally, in the first mode, the removable card **10** is connected to the USB interface **114** through the docking switch **160**. However, when the device **100** is connected to the PC **170** or through the NFC **24**, the docking switch **160** is changed causing the removable card **10** to disconnect from the USB interface **114**. Thus, for example, when a USB cable is connected to the docking switch **160**, the removable card **10** disconnects from the USB interface **114** and connects directly to the PC **170** along its USB port. The docking switch **160** then breaks the connection between the removable card **10** and the rest of the device **100** including the transceiver **104**. Because the removable card **10** contains the cellular network **110** access information, if the device **100** was accessing the Internet wirelessly through the cellular network **110**, then the device **100** would cease to transmit/receive wirelessly to/from the cellular network **110**. Similar to the first mode of operation, when the device **100** is connected to the Internet **150** through the docking switch **160**, to the PC gateway **170**, it is initially assigned a public IP address, by the Internet Service Provider (ISP) for connection to the Internet **150**. Again, this is a dynamically assigned public IP address for use during the session that the device **100** is connected to the Internet **150**.

Finally, because the removable card **10** stores a public IP address assigned by the MNO, in the user restricted portion of the memory, that public IP address directs the device **100** to the MNO server **200**. During the time period when the device **100** is connected to the Internet **150** through the PC portal **170**, and when the user is not browsing or surfing the Internet **150**, (as in e.g. when the device **100** is in the docking station connected to the docking switch **160** for charging the battery for the device **100**) the device **100** can go the MNO server **200** using the public IP address stored in the removable card **10**. The MNO server **200** can then cause content, such as movies, or programming code (updates for the device **100**) to be downloaded and stored in the user restricted portion of the removable card **10** of the device **100**. The benefit of this mode is that a large amount of content can be downloaded when the device **100** is not connected to the cellular network **110**, and when the user is not actively surfing or browsing the Internet **150**. The downloaded movies or other material can be subsequently activated by an authorization code and/or payment code. Since the movies or other content were downloaded from the MNO server **200**, the user can be sure of the trustworthiness of the content (i.e. free from virus etc.). In addition, since the owner of the content knows that the content is downloaded in a secure manner and stored in a user restricted portion, they can be assured that illicit copies will not be made. In this manner, this becomes a trustworthy procedure for all parties. Finally, by also permitting programming code to be distributed in this manner, an efficient and convenient mode is provided to assure the update of the devices **100**.

Furthermore, each removable card **10** may also be assigned a unique IP address by the MNO operator. This offers another unique feature of the present invention. When the device **100** with the removable card **10** connected thereto is connected to the Internet **150**, and with the removable card **10** having a unique IP address, the MNO server **200** which is also connected to the Internet **150** can download information for all removable cards **10** or just certain removable cards **10** or even only a specific removable card **10**. The information downloaded to one or more removable cards **10** may be stored in the user restricted memory portion of the card **10**. Examples of information that can be stored in the user restricted portion may include: administrative information such as change in calling plan, increase in minutes etc. Further, the "information" may be data or it may be programming code (including Java applets) for execution by the host controller **12**. Thus, for example, the "information" downloaded from the MNO server **200** may be a program causing the host controller **12** to execute the code causing the device **100** to access the cellular network **110** to access the Internet **150** periodically or to access specified location on the Internet **150** (such as the IP address of the MNO server **200**) or in some specified manner to retrieve updates, downloads, etc.

Because the device **100** can connect to the Internet through the common carrier network, the user may store user data in the second portion **220***b* of the memory **20**. However, since the memory **20** is accessible by the MNO, the MNO may provide services to the user such as back up for the user data stored in the second portion **220***b* of the memory **20**. However, since the user data stored in the second portion **220***b* may be personal or confidential information of the user, the user will want the user data to be secure even from the MNO, and also in the event the device **100** is lost or stolen. Referring to FIG. **6** there is shown a block level diagram of a portion of the secure removable card **10** of the present invention. The card **10** has a non-volatile memory **20** with its first portion **220***a* which has restricted access by the user, and a second portion **220***b* to which the user can store user data. The MNO can access both the first portion **220***a* and the second portion **220***b* of the memory **20**. The card **10** also has a volatile memory **250**, for storing a user supplied password. The volatile memory retains the password only when power is supplied to the card **10** or the device **100**. When the power is removed, the same password needs to be re-inputted by the user. The card **10** also comprises an encryption circuit **230**, which receives inputted user data, as well as the output of the volatile memory **250**. The encryption circuit encrypts the user data with the password and then the encrypted data is supplied to the second portion **220***b* of the memory **20** for storage. When it is desired to read the data from the second portion **220***b* of the memory **20**, the encrypted data is read from the second portion **220***b* and is supplied to a decryption circuit **240**. The decryption circuit uses the password from the volatile memory to decrypt the encrypted data and supplies the decrypted user data back to the user.

As can be seen from the foregoing the card **10** of the present invention is extremely secure. What is stored in the a second portion **220***b* is always encrypted data. Thus, even if the device **100** is lost or stolen and a would be hacker attempts to read the data from the second portion **220***b*, the hacker would find only encrypted data. The degree of security is limited only by the sophistication of the encryption circuit **130** and the number of bits of the password to encrypt the user data. Further, the encryption is active only while power is supplied. In the event the device **100** is turned off, and back on, a new session commences and the user will need to re-input the password.

Finally, in the event the user forgets the password, it should be noted that the password is not stored in any portion of the memory **20**. Thus, if the password is forgotten, the penalty is quite severe. One way to mitigate this harsh result may be to store a "hint" question or phrase (such as what's the name of your favorite pet) in the second memory **220***b*, so that the user may be prompted to recall the forgotten password. However, such "hint" may also compromise the security of the card **10**. Nevertheless, the password itself is never stored in the memory **20**.

What is claimed is:

1. A removable card having electrical connections for connecting to a mobile wireless communicating device for use by a user to access a common carrier network to access a network of interconnected computer networks ("Internet"), comprising:

a processor;

a non-volatile memory connected to the processor, having two portions: a first portion and a second portion wherein said first portion is accessible by the provider of the common carrier network with said processor restricting access thereto by the user, and wherein said second portion is accessible by the provider of the common carrier network and with said processor granting access thereto to the user for storing user data therein; and

logic circuit for encoding the user data to produce encrypted user data, wherein said encrypted data is stored in said second portion; wherein said logic circuit comprising a volatile memory for storing a user supplied password, wherein said password is stored in said volatile memory only when power is supplied to said memory;

an encryption circuit for receiving the user supplied user data and the output of the volatile memory and for encrypting said user data with said password from said volatile memory to produce encrypted user data, and for storing said encrypted user data in said second portion; and

a decryption circuit for receiving encrypted user data stored in the second portion and the output of the volatile memory and for decrypting said encrypted user data with said password from said volatile memory to produce user data.

2. The removable card of claim **1** wherein the partitioning of said first portion and said second portion is alterable.

3. The removable card of claim **1** wherein the non-volatile memory has programming code stored therein configured to be processed by the processor and operable in one of two modes: a first mode in which said card is connected to the device with the card storing information received wirelessly by the device from the Internet; and a second mode in which said card is connected to a network portal device, which is connected to the Internet, with the card storing information received through the network portal device from the Internet.

4. The removable card of claim **3** wherein in said first mode said card storing information received wirelessly by the device through a wireless network having a wireless access device connected to the Internet, and wherein in said second mode said card is connected directly to the Internet through the network portal device.

5. A mobile wireless communication device for use by a user to access a common carrier network to access a network of interconnected computer networks ("Internet") comprising:

a transceiver for communicating wirelessly via a wireless common carrier network;

a first processor for controlling communication of the device to connect to the common carrier network;

a second processor;

a non-volatile memory connected to the second processor, having two portions: a first portion and a second portion wherein said first portion is accessible by the provider of the common carrier network with said second processor restricting access thereto by the user, and wherein said second portion is accessible by the provider of the common carrier network and with said second processor granting access thereto to the user for storing user data therein; and

logic circuit for encoding the user data to produce encrypted user data for storing in said second portion; wherein said logic circuit comprising a volatile memory for storing a user supplied password, wherein said password is stored in said volatile memory only when power is supplied to said memory;

an encryption circuit for receiving the user supplied user data and the output of the volatile memory and for encrypting said user data with said password from said volatile memory to produce encrypted user data, and for storing said encrypted user data in said second portion; and

a decryption circuit for receiving encrypted user data stored in the second portion and the output of the volatile memory and for decrypting said encrypted user data with said password from said volatile memory to produce user data.

6. The device of claim **5** wherein said second processor, non-volatile memory, and logic circuit are contained in a removable card.

7. The device of claim **6** wherein the partitioning of said first portion and said second portion is alterable.

8. The device of claim **7** wherein the non-volatile memory has programming code stored therein configured to be processed by the second processor and operable in one of two modes: a first mode in which said card is connected to the transceiver with the card storing information received wirelessly by the device from the Internet; and a second mode in which said card is connected to a network portal device, which is connected to the Internet, with the card storing information received through the network portal device from the Internet.

9. The device of claim **8** wherein in said first mode said card storing information received wirelessly by the device through a wireless network having a wireless access device connected to the Internet, and wherein in said second mode said device is connected directly to the Internet through the network portal device.

* * * * *

APPENDIX
TAB C

US007519754B2

(12) United States Patent

Wang et al.

(10) **Patent No.: US 7,519,754 B2**

(45) **Date of Patent: Apr. 14, 2009**

(54) **HARD DISK DRIVE CACHE MEMORY AND PLAYBACK DEVICE**

(75) Inventors: **Jeremy Wang**, Shijr (TW); **Fong-Long Lin**, Fremont, CA (US); **Bing Yeh**, Los Altos Hills, CA (US)

(73) Assignee: **Silicon Storage Technology, Inc.**, Sunnyvale, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 140 days.

(21) Appl. No.: **11/637,419**

(22) Filed: **Dec. 11, 2006**

(65) **Prior Publication Data**

US 2007/0233933 A1 Oct. 4, 2007

Related U.S. Application Data

(60) Provisional application No. 60/754,937, filed on Dec. 28, 2005.

(51) **Int. Cl.**
G06F 13/00 (2006.01)

(52) **U.S. Cl.** **710/110**; 710/305; 710/308; 710/306; 710/311; 710/27; 365/63; 365/189.08; 712/33

(58) **Field of Classification Search** 710/110, 710/205, 306, 308, 311, 27; 712/33; 365/63, 365/189.08

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,534,011	A	*	8/1985	Andrews et al.	710/58
4,837,677	A	*	6/1989	Burrus et al.	710/308
4,860,192	A	*	8/1989	Sachs et al.	711/3
4,937,567	A	*	6/1990	Orr et al.	370/463
4,955,024	A	*	9/1990	Pfeiffer et al.	714/763

(Continued)

FOREIGN PATENT DOCUMENTS

WO	WO 2004/025474	3/2004

(Continued)

OTHER PUBLICATIONS

Lane Mason and Ivan Greenberg, Denali Memory Vendor Program—Microsoft Internet Explorer, Sponsored by Denali and Samsung Semiconductor, "Samsung OneNAND: Speeding The Next Generation Of Mobile Handset Innovation," pp. 1-28, dated Sep. 2, 2004.

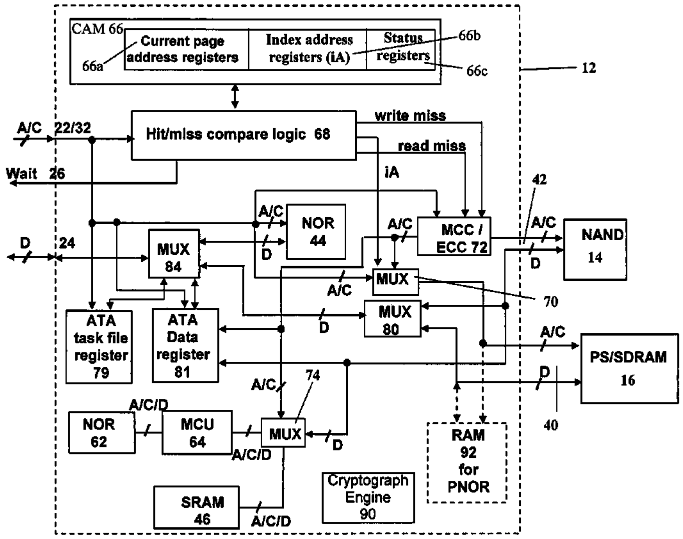
(Continued)

Primary Examiner—Viet Q Nguyen
(74) *Attorney, Agent, or Firm*—DLA Piper LLP (US)

(57) **ABSTRACT**

A NOR emulating device using a controller and NAND memories can be used in a computer system in placed of the main memory or in place of the BIOS NOR memory. Thus, the emulating device can function as a bootable memory. In addition, the device can act as a cache to the hard disk drive. Further, with the addition of an MP3 player controller into the device, the device can function as a stand alone audio playback device, even while the PC is turned off or is in a hibernating mode. Finally with the MP3 player controller, the device can access additional audio data stored on the hard drive, again with the PC in an off mode or a hibernating mode. Finally, the device can function to operate the disk drive, even while the PC is off or is in a hibernating mode, and control USB ports attached thereto.

6 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

4,965,717	A	*	10/1990	Cutts et al.	714/12
4,974,153	A	*	11/1990	Pimm et al.	710/306
5,134,706	A	*	7/1992	Cushing et al.	710/268
5,189,665	A	*	2/1993	Niehaus et al.	370/248
5,210,530	A	*	5/1993	Kammerer et al.	340/3.51
5,218,686	A	*	6/1993	Thayer	711/100
5,276,807	A	*	1/1994	Kodama et al.	710/305
5,276,823	A	*	1/1994	Cutts et al.	714/11
5,341,487	A	*	8/1994	Derwin et al.	711/146
5,379,415	A	*	1/1995	Papenberg et al.	714/5
5,404,485	A		4/1995	Ban	
5,446,869	A	*	8/1995	Padgett et al.	703/27
5,535,340	A	*	7/1996	Bell et al.	710/112
5,561,819	A	*	10/1996	Gephardt et al.	710/27
5,581,741	A	*	12/1996	Clark et al.	703/25
5,673,414	A	*	9/1997	Amini et al.	711/146
5,699,529	A	*	12/1997	Powell et al.	710/53
5,721,839	A	*	2/1998	Callison et al.	710/310
5,729,760	A	*	3/1998	Poisner	710/3
5,764,966	A	*	6/1998	Mote, Jr.	713/400
5,778,418	A		7/1998	Auclair	
5,805,792	A	*	9/1998	Swoboda et al.	714/28
5,805,835	A	*	9/1998	Jeddeloh et al.	710/107
5,905,509	A	*	5/1999	Jones et al.	345/520
5,937,425	A		8/1999	Ban	
5,955,905	A	*	9/1999	Idei et al.	327/160
5,990,914	A	*	11/1999	Horan et al.	345/531
6,016,530	A		1/2000	Auclair	
6,029,253	A	*	2/2000	Houg	713/600
6,088,822	A	*	7/2000	Warren	714/726
6,098,110	A	*	8/2000	Witkowski et al.	709/249
6,199,137	B1	*	3/2001	Aguilar et al.	710/305
6,199,167	B1	*	3/2001	Heinrich et al.	726/18
6,223,279	B1	*	4/2001	Nishimura et al.	712/228
6,330,635	B1		12/2001	Stafford	
6,415,353	B1	*	7/2002	Leung	711/106
6,421,765	B1		7/2002	Poisner	
6,456,517	B2		9/2002	Kim et al.	
6,502,146	B1	*	12/2002	Rasmussen et al.	710/100
6,510,488	B2		1/2003	Lasser	
6,633,944	B1	*	10/2003	Holm et al.	710/306
6,636,935	B1	*	10/2003	Ware et al.	711/5
6,658,006	B1	*	12/2003	Chen et al.	370/395.1
6,813,673	B2	*	11/2004	Kotlowski et al.	710/305
6,871,253	B2	*	3/2005	Greeff et al.	710/316
6,882,082	B2	*	4/2005	Greeff et al.	310/307
6,934,785	B2	*	8/2005	Lee et al.	710/300
7,127,549	B2		10/2006	Sinclair	
7,136,973	B2		11/2006	Sinclair	
7,334,107	B2	*	2/2008	Schoinas et al.	711/207
2002/0185337	A1		12/2002	Miura et al.	
2003/0050087	A1		3/2003	Kwon	
2003/0156454	A1		8/2003	Wei et al.	
2003/0206442	A1		11/2003	Tang et al.	
2004/0049629	A1		3/2004	Miura et al.	
2004/0064606	A1		4/2004	Kimura	
2004/0139310	A1		7/2004	Maeda et al.	
2005/0204091	A1		9/2005	Kilbuck et al.	
2006/0041711	A1		2/2006	Miura et al.	
2006/0053246	A1		3/2006	Lee	

FOREIGN PATENT DOCUMENTS

WO	WO2004/049168	6/2004
WO	WO2005/076137	8/2005

OTHER PUBLICATIONS

Anu Murthy and Brian Gardner, Denali Memory Vendor Program—Microsoft Internet Explorer, Sponsored by Denali and Samsung Semiconductor, "Ultra-Fast Controller For An Ultra-Fast Flash Device—Extracting All of One-NAND Performance," pp. 1-51, Aug. 17, 2005.

Don Barnetson, Samsung Semiconductor, Inc., "OneNAND Bridge or Destination," pp. 1-8, Sep. 22, 2005.

M-Systems, Flash Disk Pioneers, "DiskOnChip G3 Low Power (LP) 64MB (512Mb)—Flash Disk With 1.8V Core and I/O," pp. 1-62, 91-DT-0904-20, dated Sep. 2004; and "Big/Little Endian Byte Order," pp. 6-20, AP-DOC-0504, Rev. 1.0.

M-Systems, Flash Disk Pioneers, "DiskOnChip H1 4Gb (512MBYTE) and 8Gb (1GByte) High Capacity Flash Disk With NAND and x2 Technology," pp. 1-66, 95-DT-1104-01, dated 2005.

M-Systems DiskOnChip, "On-Board Embedded Flash Drive," Binder with several articles, datasheets and other documents, 2006.

Korean Intellectual Property Office Notice of Preliminary Rejection dated Feb. 29, 2008 corresponding to the related Korean Patent Application No. 2006-0136569.

PRC's First Office Action (English Version) dated Apr. 11, 2008 including the cited Chinese references (Chinese Version) corresponding to the related Chinese Patent Application No. 200610064390.4.

PCT International Preliminary Examination Report (English Version), published International Patent Application No. WO 2004/049168 A1 (Japanese Version), PCT Search Report (Japanese Version) in connection with PCT Patent Application No. JP2003/015165.

PCT International Preliminary Examination Report, published International Patent Application No. WO 2005/076137 A1, PCT Written Opinion and Search Report in connection with PCT Patent Application No. CA2005/000137.

European Search Report dated Oct. 18, 2007 corresponding to the related European Patent Application No. 06026552.7-2212.

* cited by examiner

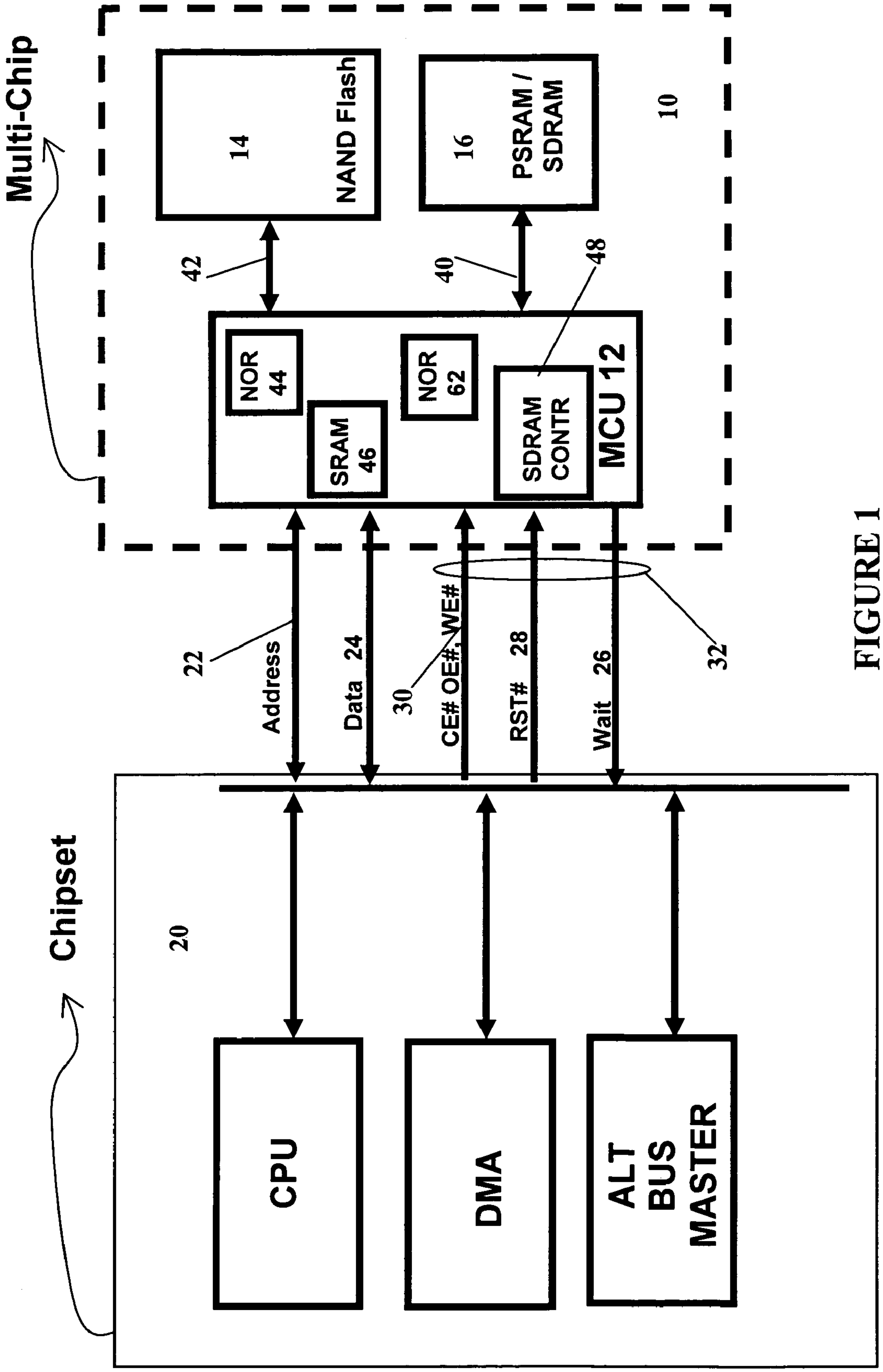

Multi-Chip
10
14
NAND Flash
16
PSRAM / SDRAM
42
40
48
NOR 44
SRAM 46
NOR 62
SDRAM CONTR
MCU 12
22
Address
Data 24
30
CE# OE#, WE#
RST# 28
Wait 26
32
Chipset
20
CPU
DMA
ALT BUS MASTER

FIGURE 1

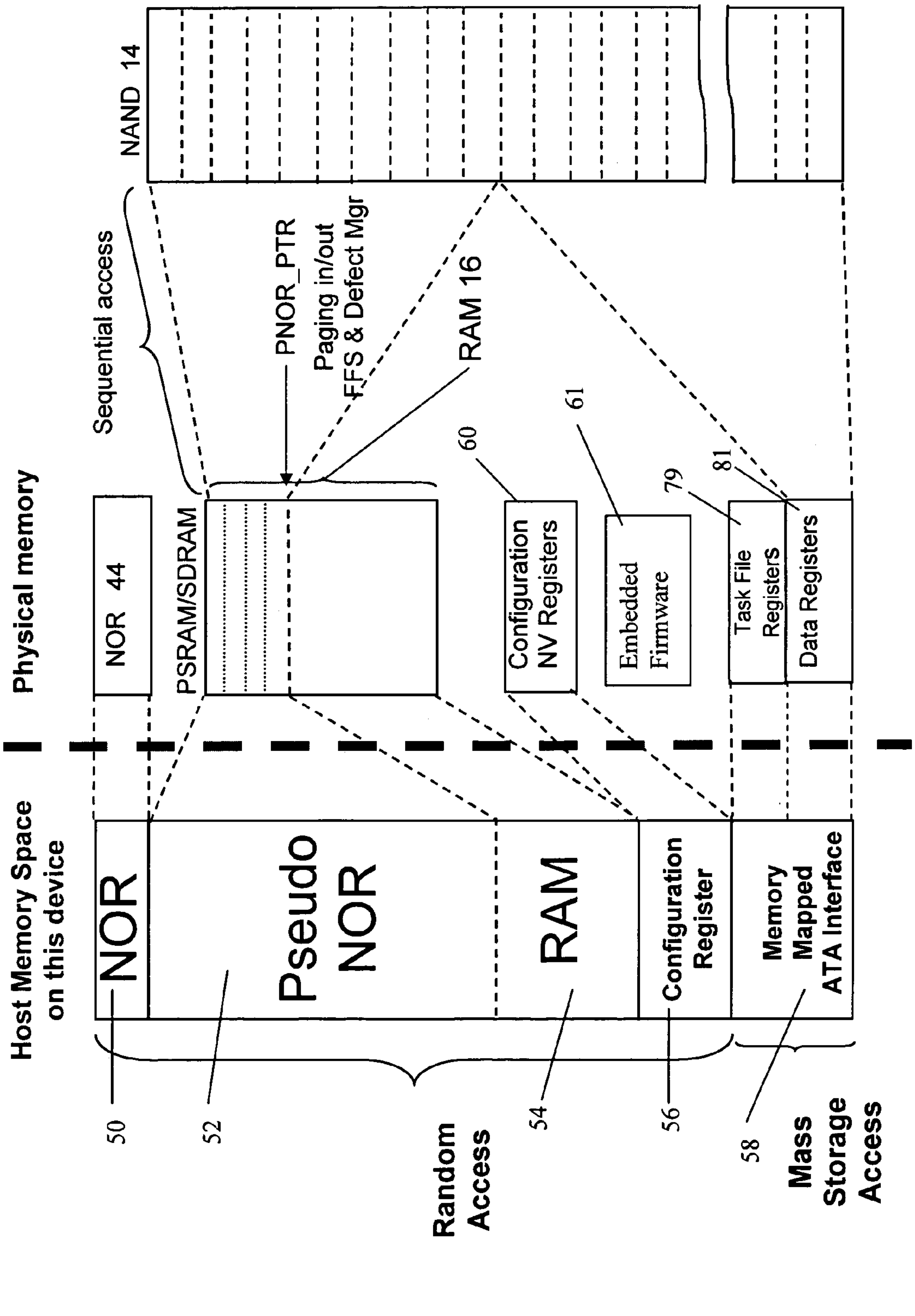

Host Memory Space on this device
NOR
Pseudo NOR
RAM
Configuration Register
Memory Mapped ATA Interface
50
52
54
56
58
Random Access
Mass Storage Access
Physical memory
NOR 44
PSRAM/SDRAM
Configuration NV Registers
Embedded Firmware
Task File RegisterS
Data Registers
60
61
79
81
Sequential access
PNOR_PTR
Paging in/out
FFS & Defect Mgr
RAM 16
NAND 14

Figure 2

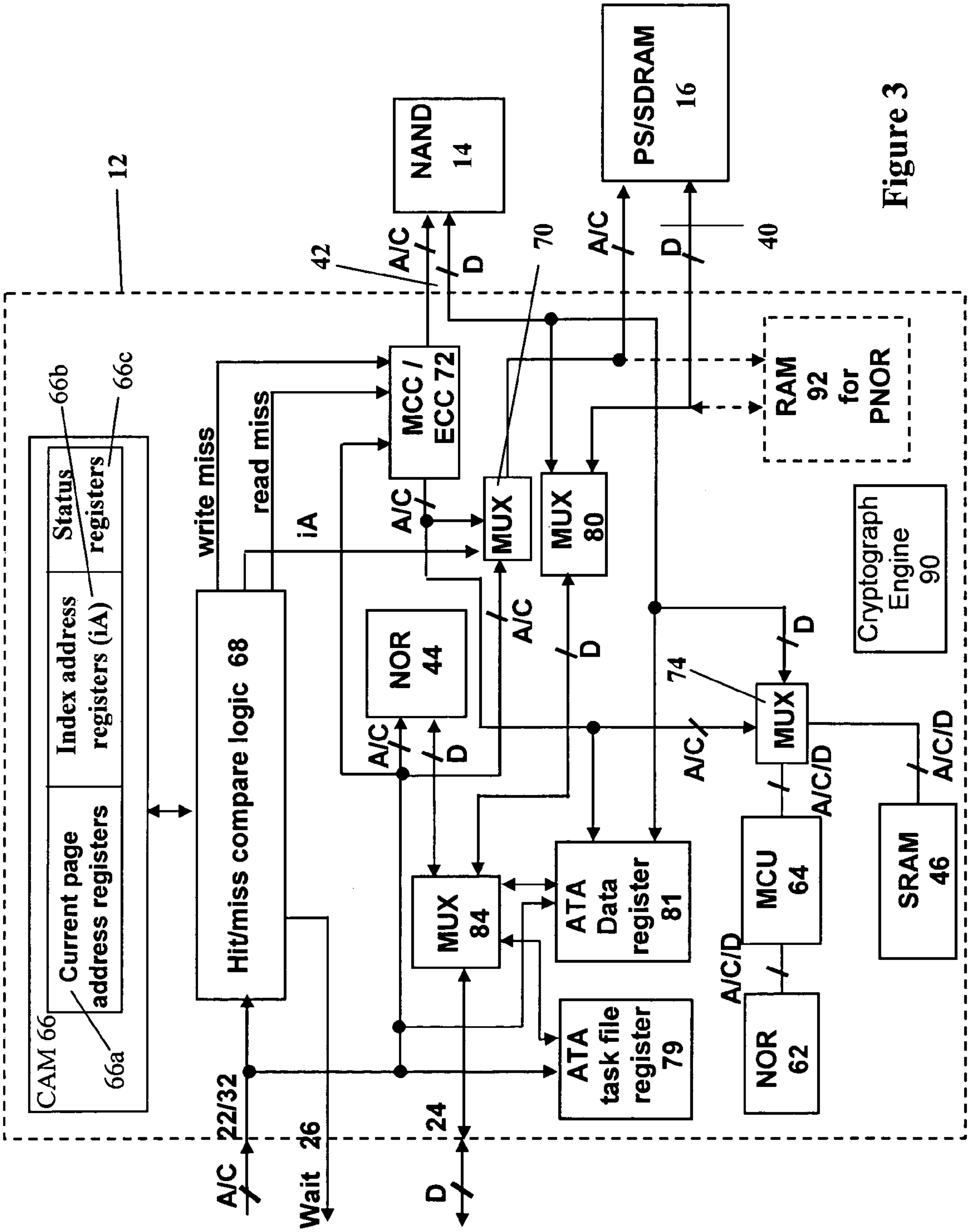

12
CAM 66
Current page address registers
66a
Index address registers (iA)
66b
Status registers
66c
Hit/miss compare logic 68
write miss
read miss
iA
MCC / ECC 72
NAND 14
PS/SDRAM 16
42
A/C
D
70
40
MUX
MUX 80
RAM 92 for PNOR
NOR 44
A/C
D
74
MUX
Cryptograph Engine 90
A/C/D
MUX 84
ATA Data register 81
ATA task file register 79
MCU 64
SRAM 46
NOR 62
22/32
Wait 26
24

Figure 3

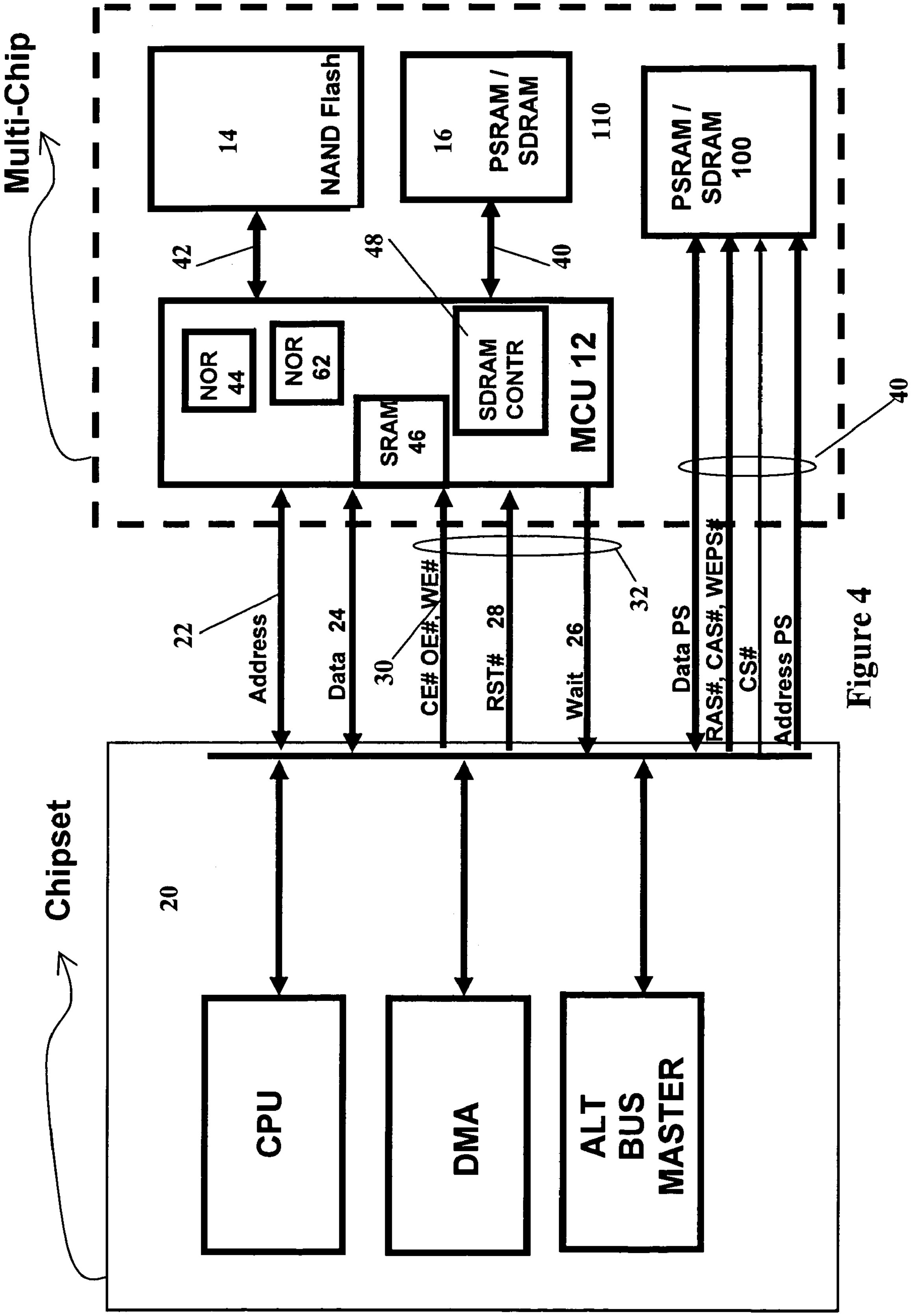

Multi-Chip
14
NAND Flash
16
PSRAM / SDRAM
110
PSRAM / SDRAM 100
42
48
40
NOR 44
NOR 62
SRAM 46
SDRAM CONTR
MCU 12
40
22
Address
Data 24
30
CE# OE#, WE#
RST# 28
Wait 26
32
Data PS
RAS#, CAS#, WEPS#
CS#
Address PS
Chipset
20
CPU
DMA
ALT BUS MASTER

Figure 4

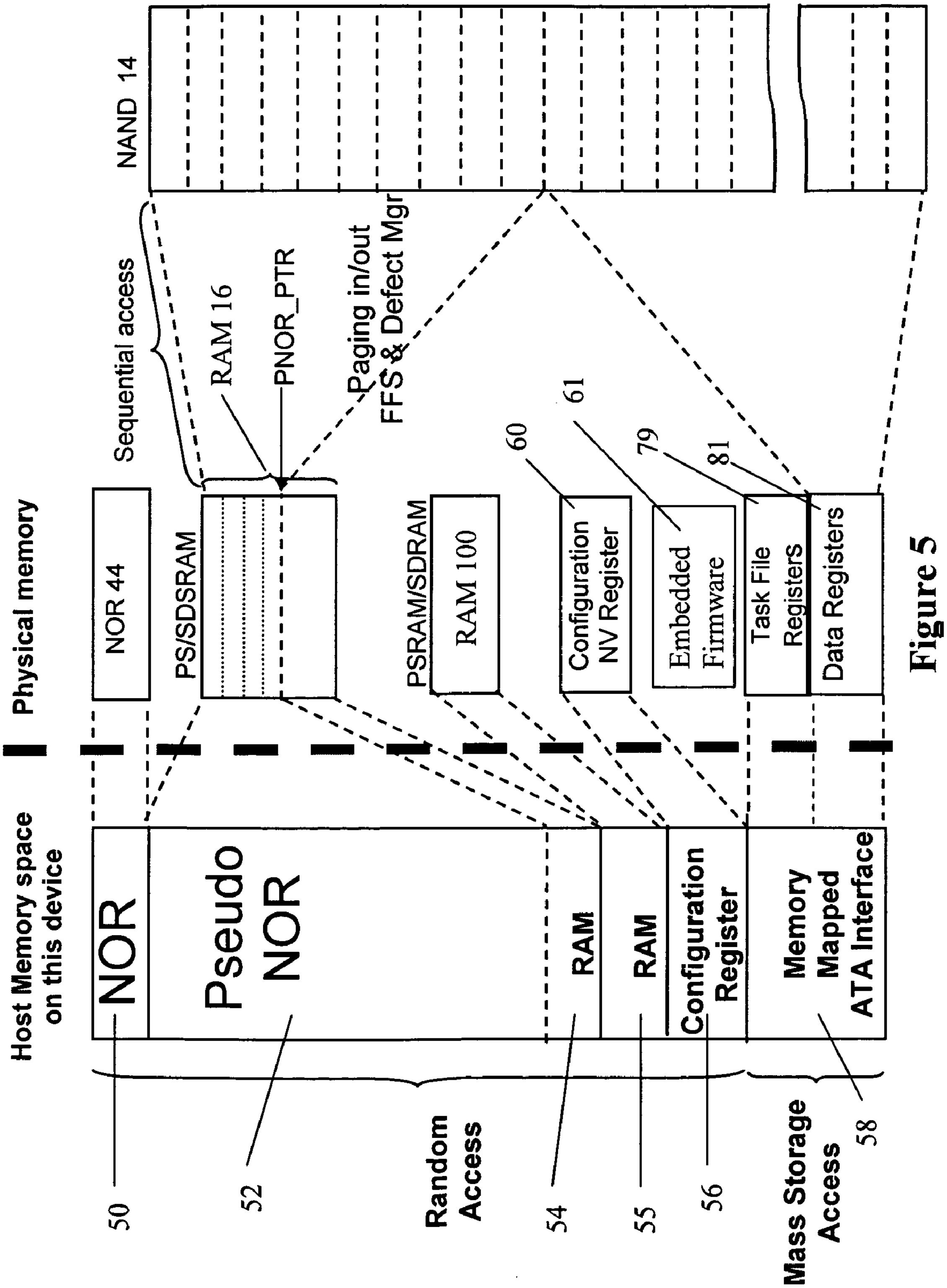

Host Memory space
on this device
Physical memory
NOR
Pseudo
NOR
RAM
RAM
Configuration
Register
Memory
Mapped
ATA Interface
50
52
Random
Access
54
55
56
Mass Storage
Access
58
NOR 44
PS/SDSRAM
PSRAM/SDRAM
RAM 100
Configuration
NV Register
Embedded
Firmware
Task File
Registers
Data Registers
60
61
79
81
Sequential access
RAM 16
PNOR_PTR
Paging in/out
FFS & Defect Mgr
NAND 14

Figure 5

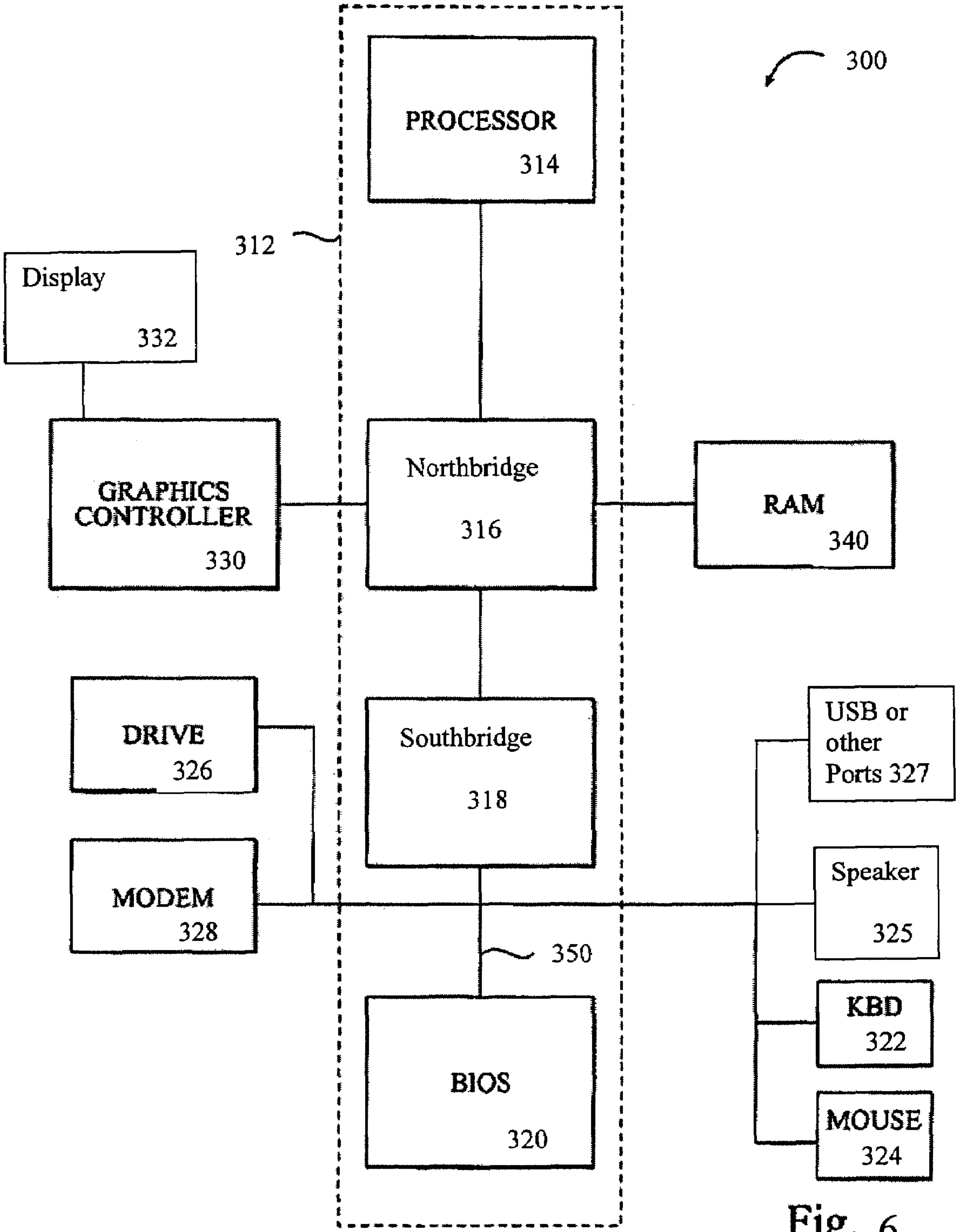


Fig. 6

(Prior Art)

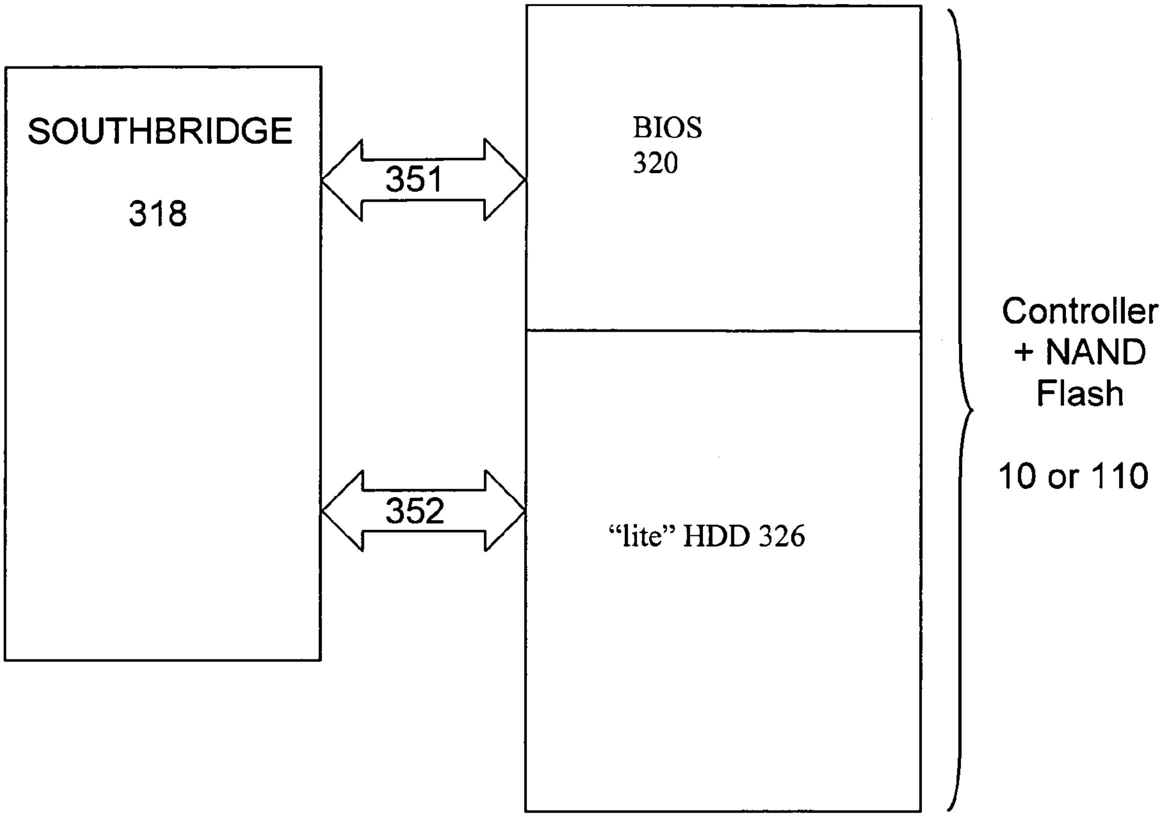

SOUTHBRIDGE
318
351
352
BIOS
320
"lite" HDD 326
Controller
+ NAND
Flash
10 or 110

Figure 7A

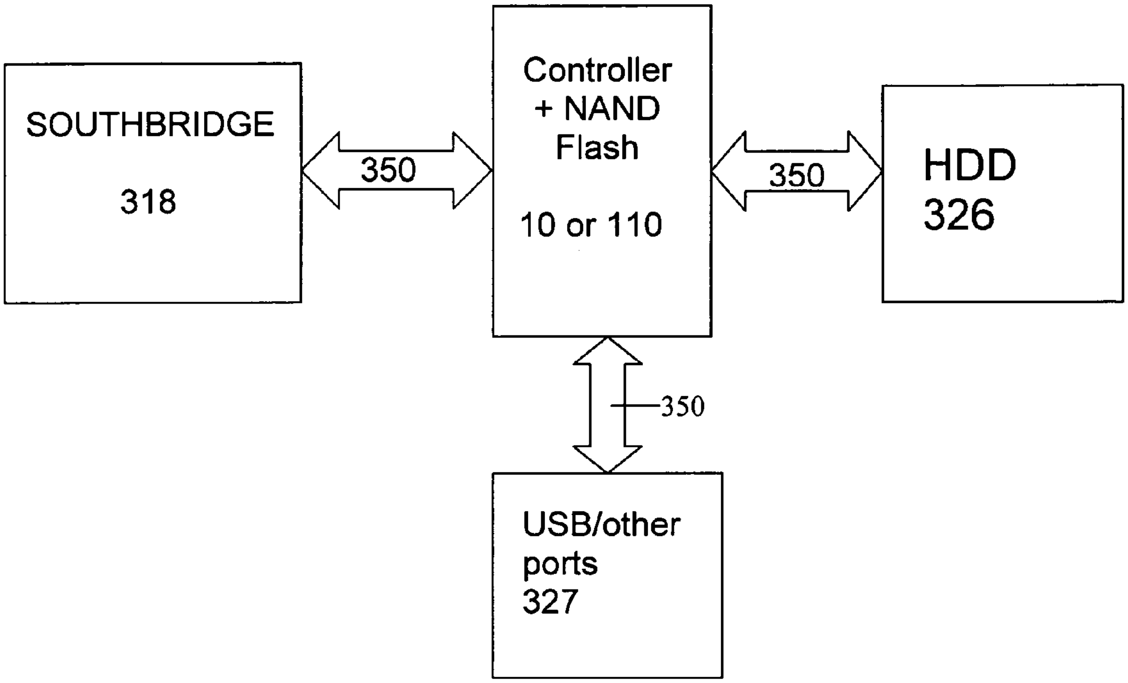


Figure 7B

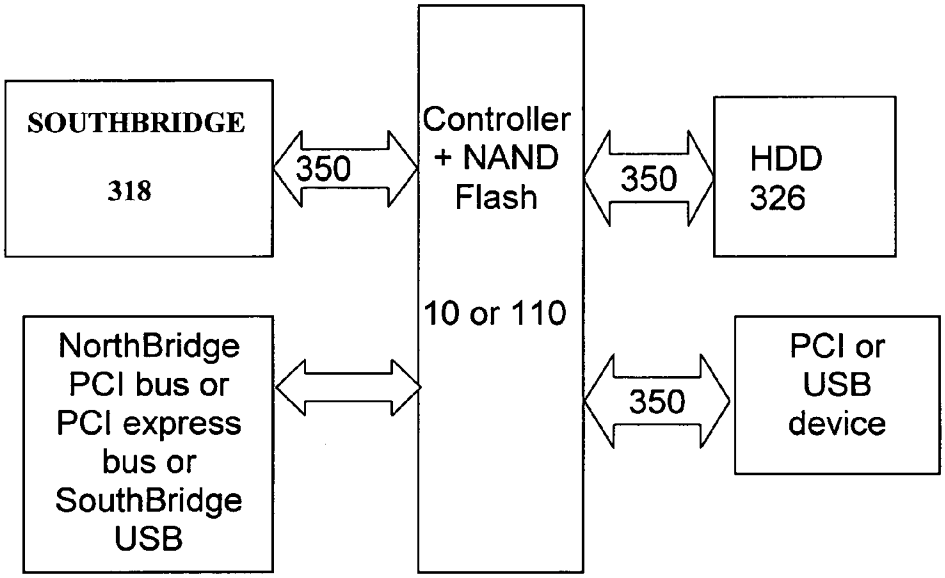


Figure 7C

HARD DISK DRIVE CACHE MEMORY AND PLAYBACK DEVICE

This application claims the priority of a provisional application 60/754,937 filed on Dec. 28, 2005, whose disclosure is incorporated herein in its entirety.

TECHNICAL FIELD

The present invention relates to a memory device and more particularly to a memory device for use as a disk drive cache memory in a personal computer, such as a PC, and can also function as a playback device for play back of music or video while the PC is either in a hibernating mode or even off mode.

BACKGROUND OF THE INVENTION

Volatile random access memory, such as SRAM or DRAM (or SDRAM) or PSRAM (hereinafter collectively referred to as RAM), are well known in the art. Typically, these types of volatile memories receive address signals on an address bus, data signals on a data bus, and control signals on a control bus.

Parallel NOR type non-volatile memories are also well known in the art. Typically, they receive address signals on the same type of address bus as provided to a RAM, data signals on the same type of data bus as that provide to a RAM, and control signals on the same type of control bus as that provided to a RAM. Similar to a RAM, NOR memories are a random access memory device. However, because NOR memories require certain operations, not needed by a RAM, such as SECTOR ERASE or BLOCK ERASE, the operations, which are in the nature of commands, are provided to the NOR device as a sequence of certain data patterns. This is known as NOR command protocols. In the prior art, there are two types of NOR command protocols: 1) those protocol commands that are compatible with the protocol command set initially promulgated by Intel, and 2) those protocol commands that are compatible with the protocol command set initially promulgated by AMD. In either event, a NOR memory interfaces electrically to the same address, data and control buses as a RAM interfaces with. Furthermore, conventional NOR memory devices may also provide data, address, and control signals serially, in well known conventional formats such as SPI, LPC or firmware hub.

NAND type non-volatile memories are also well known in the art. Unlike parallel NOR devices, however, NAND memories store data in random accessible blocks in which cells within a block are stored in a sequential format. Further, address and data signals are provided on the same bus, but in a multiplexed fashion. NAND memories have the advantage that they are more dense than NOR devices, thereby lowering the cost of storage for each bit of data.

Because of the lower cost per bit of data for a NAND device, there has been attempts to use a NAND device to emulate the operation of a NOR device. One such device called OneNAND (trademark of Samsung Corporation) uses a RAM memory to temporarily buffer the data to and from a NAND memory, thereby emulating the operation of a NOR memory. However, it is believed the OneNAND device suffers from two shortcomings. First, it is believed that the user or the host device which interfaces the OneNAND must keep track of the data coherency. In data coherency, because the user or host writes to the RAM, the data in the RAM may be newer (and therefore different from the) data in the location in the NAND from which the data in the RAM was initially read. Thus, in the OneNAND device the user or the host must act to write data from the RAM back to the ultimate location in the NAND to store that data, or to remember that the data in the RAM is the newer data. A second problem is believed to be a shortcoming of the OneNAND device is that it cannot provide for automatic address mapping. In the OneNAND device, once data is written into the RAM portion of the OneNAND device, the host or the user must issue a command or series of commands to write the data in the RAM portion to the ultimate location in the NAND portion of the OneNAND device. Similarly, for a read operation, the host or user must issue a read command from specified location(s) in the NAND portion of the OneNAND to load that data into the RAM portion, and then read out the data from the RAM portion.

Another prior art device that is believed to have similar deficiency is the DiskOnChip device from M Systems. In the DiskOnChip device, a thin controller with a limited amount of RAM controls the operation of NAND memories. However, it is believed that the controller portion of the DiskOnChip device does not have any on board nonvolatile bootable memory, such as NOR memory.

A prior art publication showing the use of NAND memories with a controller emulating NOR memory operation is shown in US patent application 2006/0053246, published Mar. 9, 2006. Although this publication shows the use of NAND memories with controller connected to a plurality of processors, it appears that the NAND memory cannot be accessed directly through an ATA format operation. Thus, all access to the NAND memory must be accomplished by the controller with no direct access from the external.

Computer systems are well known in the art. In particular, a computer system adhering to the "IBM PC" standard is well known in the art. Referring to FIG. **6**, there is shown a computer system **300** of the prior art. The computer system **300** conforms to the "IBM PC" architecture. The system **300** comprises typically a motherboard **312** on which are mounted a variety of components such as a processor **314**, such as a Pentium microprocessor made by Intel Corporation, a memory controller hub chip **316**, also known as Northbridge chip **316** and a IO controller hub chip **318**, also known as Southbridge chip **318**. The Northbridge **316** and the Southbridge **318** are known as chipsets and can be obtained from Intel Corporation. Finally, the motherboard **312** comprises a BIOS **320** which is typically a NOR type non-volatile memory device, which is connected to the Southbridge **318** via a bus **350**. The bus **350** is also connected to other components of the system **300**, such as Hard Disk Drive (HDD) **326**, Modem **328**, USB or other ports **327**, speaker **325**, Keyboard **322** and mouse **324**. The foregoing system is described and is disclosed in U.S. Pat. No. 6,421,765. See also U.S. Pat. No. 6,330,635.

In the operation of the computer system **300**, the processor **314**, boots up from the code that is initially stored in the BIOS **320**. Once the processor **314** has executed the initial code from the BIOS **320**, it sends signals to the HDD **326** to retrieve further code/data stored on the HDD **326**. Thereafter, the operation continues.

As can be seen from the foregoing, if the drive **326** is activated, the processor **314** and the entire system **300** must be "on." With battery time on a lap top computer **300** at a premium, it is desired to conserve battery power. Further, it is desired to improve the performance of such a system **300**. Accordingly, there is a need for an improved device that can satisfy the foregoing.

SUMMARY OF THE INVENTION

In the present invention, a novel memory device is disclosed. The novel memory device uses NAND flash memories to emulate the function of a NOR memory. Further, the memory device is used in a PC system to replace the volatile DRAM or to be used as a bootable BIOS memory. In addition, the memory device can act as a cache to the hard disk drive. Further, the memory device can act as a hub for USB devices thereby controlling the transfer of data to/from the hard disk drive, even while power is off to the main processor. Further, since the memory device has a controller, the controller can perform other functions (or a dedicated processor, such as DSP, can also be used) such as MP3 playback. Thus, the memory device can function as a stand alone audio playback device, even while the PC is turned off or is in a hibernating mode. Finally with the MP3 player controller, the memory device can access additional audio data stored on the hard drive, again with the PC in an off mode or a hibernating mode.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block level diagram of a first embodiment of a memory device, including the memory controller, connected to a host system or user.

FIG. **2** is a memory mapping diagram showing the mapping of the address space as seen-by the host or the user, external to the memory device of FIG. **1**, to the NOR memory, the RAM memory and the NAND memory in the first embodiment of the memory device shown in FIG. **1**.

FIG. **3** is a detailed block level circuit diagram of the controller, used in the memory device of FIG. **1**.

FIG. **4** is a block level diagram of a second embodiment of a memory device, including the memory controller, connected to a host system or user.

FIG. **5** is a memory mapping diagram showing the mapping of the address space as seen by the host or the user external to the memory device of FIG. **4** to the NOR memory, the RAM memory and the NAND memory in the second embodiment of the memory device, shown in FIG. **4**.

FIG. **6** is a block level diagram of a computer system in accordance with the "IBM PC" architecture of the prior art.

FIGS. **7***a*, **7***b* and **7***c* are block level diagrams showing the connection and use of a memory device in accordance with either the first or second embodiment with components of the "IBM PC" shown in FIG. **6**.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. **1**, there is shown a first embodiment of a memory device **10**. The memory device **10** comprises a memory controller **12**, a NAND memory **14**, and a RAM memory **16**. The memory device **10** interfaces with a host device **20**, through a first RAM address bus **22**, a first RAM data bus **24**, and a plurality of control signals such as wait **26**, RST# **28**, and CE#, OE#, and WE# **30**, all of which are well known to one skilled in the art of control signals for a RAM bus. Hereinafter unless otherwise specified, all of the control signals on the wait **26**, RST# **28** and CE#, OE# and WE# **30** are referred to as first RAM control bus **32**. The first RAM address bus **22**, the first RAM data bus **24** and the first RAM control bus **32** are connected from the host device **20** to the memory controller **12** of the memory device **10**. Further, as discussed previously, the interface between the memory device **10** and the host device **20** can be via a serial bus in which the data, address and control buses are serially connected between the host device **20** and the memory device **10**. Such a memory device **10** is also within the scope of the present invention.

The memory controller **12** has a second RAM address bus (similar to the first RAM address bus **22**), a second RAM data bus (similar to the first RAM data bus **24**), and a second control bus (similar to the first RAM control bus **32**) all of which are collectively shown as simply as a second RAM bus **40**, connected to the RAM memory **16**. The memory controller **12** further has a NAND address/data bus and a NAND control bus (all of which are collectively shown as a NAND bus **42**) connected to a NAND memory **14**. The RAM memory **16** can be integrated or embedded in the memory controller **12**, as a single chip integrated circuit. Alternatively, the RAM memory **16** can be an integrated circuit separate from the memory controller **12**. Alternatively, portions of the RAM memory **16** can be integrated with the memory controller **12** and portions of the RAM memory **16** can be separated from the memory controller **12**. The advantage of the RAM memory **16** being a separate die will be discussed hereinafter. However, the advantage of the RAM memory **16** being integrated with the memory controller **12** is that the RAM memory **16** may be faster in operation.

In one embodiment, the memory controller **12** is a single integrated circuit die. The controller has also a first NOR memory **44**, a second NOR memory **62**, a SRAM memory **46**, and SDRAM controller **48** (for controlling the operation of the RAM **16**, if the RAM **16** is an SDRAM type of RAM memory, and is external to the memory controller **12**) embedded within the memory controller integrated circuit die. Of course, the first NOR memory **44** and the second NOR memory **62** may be a part of the same physical NOR memory. A detailed block level diagram of an embodiment of the memory controller **12** is shown in FIG. **3**. As used herein a "NOR memory" means any type of randomly accessed non-volatile memory. The NOR memory includes but is not limited to floating gate type memory, ROM, or cells using trapping material etc. Further as used herein "NAND memory" means any type of serially accessed non-volatile memory that may contain defective cells.

In one embodiment, each of the memory controller **12**, the RAM memory **16** and the NAND memory **14** is made of a single integrated circuit die and are packaged together in a MCP (Multi-Chip Package). The advantage of such an arrangement is that for a user or host **20** that requires a large (or small) amount of memory, the amount of memory can be changed by simply changing the readily available die for the NAND memory **14** or if speed is a factor then changing the readily available RAM memory **16**. Thus, having the memory controller **12**, the RAM memory **16** and the NAND memory **14** in separate dies means that-different sizes of the memory device **10** and speed or performance can easily manufactured.

Of course, the memory controller **12**, the RAM memory **16** and the NAND memory **14** can also be made into a single integrated circuit die. If the memory controller **12**, the RAM memory **16** and the NAND memory **14** are made of a single integrated circuit die, then provision can also be made to provide an external NAND bus **42** so that additional externally provided NAND memories can be attached to the memory device **10** to expand the memory capacity of the memory device **10**.

Referring to FIG. **2** there is shown a memory map showing the mapping of addresses as seen by the host device **20** and as mapped to in the first embodiment of the memory device **10** shown in FIG. **1**. The memory map as seen by the host device **20** has two general sections: Random Access and Mass Storage Access. The Random Access section occupies the lower memory address location (although that is not a requirement). Within the Random Access section, the lowest memory address is that for NOR memory access portion **50**, followed by a Pseudo NOR (PNOR) memory access portion **52**, followed by a RAM access portion **54**, followed by a configuration access portion **56**. Each of the portions will be explained as follows.

The NOR memory access portion **50** as seen by the host device **20** is that when the host **20** operates in this portion **50**, the result is an operation on the physical NOR memory **44**. Thus, the mapping of the memory portion **50** to the physical NOR memory **44** is a one-to-one. In other words, the amount of memory space allocated to the NOR portion **50** depends upon the amount of NOR memory **44** that is available in the memory device **10**. In one embodiment, the amount of NOR memory **44** embedded in the memory controller **12** is 4 Megabits, with 2K Word sector size and with 32K Word Block size. Further, when the host device **20** believes it is operating on the NOR portion **50** (as in issuing commands of read/write/erase etc.), the resultant operation is directly on the NOR memory **44**. This NOR portion **50** can be used by a host device **20** seeking to store performance critical code/data that requires random access with no latency. Further, if a program is stored in the NOR memory **44**, it can be executed in place within the NOR memory **44**. Thus the NOR memory **44** can store program or code that "boots" the host device **20**.

The PNOR portion **52** as seen by the host device **20** is that when the host **20** operates in this portion **52**, the host **20** believes it is operating on RAM memory **16** which is non-volatile. Therefore, to the host device **20**, it can operate on the PNOR portion **52** like any other RAM memory **16** except the data stored in the PNOR portion **52** is non-volatile, all without issuing NOR protocol commands. In one embodiment, the PNOR portion **52** is divided into pages, just like a NAND memory, with each page either 8K Byte, 2K Byte, or 512 Byte. In operation, when the host device **20** interfaces with the memory device **10**, it interfaces with the RAM memory **16**, with the memory controller **12** "backing up" the data to and from the NAND memory **14**, and maintaining data coherence between the RAM memory **16** and the NAND memory **14**, and with the memory controller **12** mapping the address supplied by the host device **20** to the address of the actual data in the NAND memory **14**. Because there is a larger amount of NAND memory **14** available than actual RAM memory **16**, the PNOR portion **52** can be much larger memory space than the actual amount of memory available in the RAM memory **16**.

Further, the PNOR portion **52** can be divided into four (4) regions, each mapped to a zone: zone **0**, zone **1**, zone **2** and zone **3** in the RAM memory **16**. Each zone can have a different degree of mapping. Where the mapping from a region in the PNOR portion **52** to a zone in the RAM memory **16** is one-to-one, then this is called "static paging mode." Where the mapping from a region in the PNOR portion **52** to a zone in the RAM memory **16** is many-to-one, then this is called "dynamic paging mode." A static paging mode mapping will result in the lowest latency in that the amount of memory space in the PNOR portion **52**, e.g. 256 pages (or 512K bytes in the case of 2K byte pages) is always mapped to the same amount of memory space in the RAM **16**, e.g. 256 pages (or 512K bytes), which is in turn mapped into 256 pages (or 512K bytes) in the NAND memory **14**. In that event, although there is no latency in access during operation because the RAM memory **16** is also random access, there is latency in initial load and storage from and to the NAND memory **14** to and from the RAM memory **16**. In a dynamic paging mode mapping, such as mapping 40,000 pages of the memory space in the PNOR portion **52** mapped to 512 pages of RAM memory **16**, which in turn is mapped to 40,000 pages of NAND memory **14**, a larger amount of latency will occur. This latency will occur both in the initial loading of the data/program from the NAND memory **14** into the RAM **16**, as well as during operation of retrieving data/program from the PNOR portion **52**, which may require data/program to be first loaded into the RAM **16** from the NAND memory **14**, if there is a cache miss. Thus, the latency for the PNOR portion **52** will differ depending upon the size of the zones configured. The boundary of each zone of the RAM memory **16**, and therefore, how much memory space is mapped from each region of the PNOR portion **52** into the RAM memory **16** can be set by the host device **20** or the user. As a result the host device **20** can configure the four zones to operate either in a static paging mode to store/retrieve program or time critical data, or to operate in a dynamic paging mode to store/retrieve program or data that is not time critical, with result that there is a latency if there is a cache miss.

In the event a zone is configured for static paging mode, data read coherence is not an issue, since the same amount of memory space in the PNOR portion **52** is always mapped to the same amount of space in the RAM memory **16**. However, data write coherence must still be performed. However, in the event a zone is configured for dynamic paging mode, data coherence must be provided. The host device **20** can configure the zone to operate in one of two cache coherence modes. In a first mode, the host device **20** initiates the cache coherence mode. In this mode, the host device **20** flushes the cache operation in the RAM memory **16** as and when needed by the host device **20**. In a second mode, the memory controller **12** initiates the cache coherence mode, by flushing the cache operation in the RAM memory **16** as and when needed by the memory controller **12** to maintain the coherence of the data between the cache in the RAM memory **16** and the NAND memory **14**.

Once the amount of memory space for the PNOR portion **52** and their mapping to the RAM memory **16** is set by the user, the remainder of the available memory space in the RAM memory **16** is available to be used for RAM memory access portion. The RAM memory access portion **54** as seen by the host device **20** is that when the host **20** operates in this portion **54**, the result is an operation on the physical RAM memory **16**. Thus, the mapping of the memory portion **54** to the physical RAM memory **16** is a one-to-one. Further, the amount of memory space allocated to the RAM portion **54** depends upon the total amount of RAM memory **16** that is available in the memory device **10**, and the degree of mapping of the memory space portion of the PNOR memory **52** to the RAM memory **16**. When the host believes it is operating on the RAM portion **54** (as in issuing commands of read/write etc.), the resultant operation is directly on the RAM memory **16**. This RAM portion **54** can be used by a host device **20** seeking to use the memory space as a buffer area. Since the mapping of the memory space of the PNOR portion **52** to the RAM memory **16** in each zone can be set by the user, and the total amount of RAM memory **16** is known, the boundary between the PNOR portion **52** and the RAM portion **54** is indirectly set by the user. Thus, if it is desired to have a large amount of buffer, a larger amount of the RAM portion **54** can be allocated, by decreasing the mapping between the PNOR portion **52** and the RAM memory **16** in one or more of the zones. In addition, the boundary between the PNOR portion **52** and the RAM portion **54** can be changed during operation of the memory device **10**, by resetting the memory controller **12**, and re-establishing the mapping between the memory space of the PNOR portion **52** and the RAM memory **16**, in each zone.

The boundaries for the memory map for each of the zones of the RAM memory **16** and the size of the memory space of the PNOR portion **52** can be pre-assigned and stored in the non-volatile configuration registers **60** in the memory controller **12**. Access to the configuration registers **60** is through the configuration access portion **56**. The non-volatile configuration registers **60** may be a part of the embedded NOR memory **62**. Alternatively, the boundaries for the memory map for each of the zones of the RAM memory **16** and the size of the memory space of the PNOR portion **52** can be selected by a user through one or more chip select pins. In that event, as the memory controller **12** is powered up, the boundaries for the different memories can be re-set. The NOR memory **62** can also store the firmware code **61** used for execution by the memory controller **12**, during boot up and for operation of the memory controller **12** and the MCU **64**.

Finally, in the Mass Storage Access section **58**, when the host device **20** accesses that section of the memory space, the host device **20** believes that it is accessing an ATA disk drive. The memory controller **12** translates the logical ATA disk drive space addresses, into a NAND memory **14** physical space address using the well known Flash File System (FFS) protocol. In one embodiment, for a read operation, the beginning portion of the Mass Storage Access section **58** consists of a 16 byte logical address which is loaded into the ATA Task File Register **79**. The memory controller **12** decodes the 16 bytes of task command and logical address and converts it into a physical address for accessing a particular "page" within the NAND memory **14**. The page of 512 bytes from a page in the NAND memory **14** is read and is then loaded into the Data Registers **81**, where they are accessed by the host device **20**, either sequentially or randomly. For a write operation, the reverse occurs. The logical address of where the 512 bytes of data are to be stored are first loaded into the Task File Registers **79**. A write command is written into the Task File Register **79**. The memory controller **12** decodes the command in the Task File Registers as a write command and converts it into a physical address to access the particular page in the NAND memory **14**, and stores the 512 bytes in the Data Registers **81** at that location. In another embodiment, there may be two data registers **81**(*a* & *b*) (not shown) in a so-called ping-pong configuration. In that event, one of the Data Registers **81***a* is used to supply 512 bytes of data to the host device **20** with data previously loaded from one page of the NAND memory **14**, while the other Data Register **81***b* is used to load data from another page of the NAND memory **14** into the Data Register **81***b*, to supply the data to the host device **20** after the data from the Date Registers **81***a* have been completely read out. In this manner, continuous read operation across many of pages of data from the NAND memory **14** can occur. The Data Registers **81**(*a* & *b*) can also be used in a ping-pong fashion for a write operation, so that many continuous pages of data can be written into the NAND memory **14** with little or no latency set up time.

As previously discussed, the interface between the memory device **10** and the host device **20** can be via a serial bus. In particular, such a serial bus might connect the NOR or PNOR area of the memory device **10** with the host device **20** with a conventional parallel bus connecting the RAM portion of the memory device **10** with the host device **20**.

Referring to FIG. **3** there is shown a detailed block level diagram of the memory controller **12** interfaced with the RAM memory **16** and the NAND memory **14**. The memory controller **12** comprises a microcontroller **64**. The microcontroller **64** performs or executes all bookkeeping functions of the FFS. In addition, it performs or executes Defect Management (DM) and cache data coherence algorithms, and cache flush replacement algorithms. Finally, the microcontroller **64** performs or executes cache paging scheme algorithms. All of these operations are accomplished by firmware or program code **61** stored in the NOR memory **62**, including the boot up operation or the initialization of the memory controller **12**.

The microcontroller **64** is connected to a second NOR memory **62**, which as previously discussed also stores the firmware **61** for execution by the microcontroller **64**. In addition to storing the non-volatile configuration registers **60**, the NOR memory **62** also stores the firmware for operations of FFS and DM.

The microcontroller **64** also interfaces with the SRAM memory **46** through the MUX **74**. The SRAM memory **46** serves as a local high speed buffer for the microcontroller **64** to store runtime data. In addition, the SRAM memory **46** can store defect map cache, and FFS data structure.

Although, the detailed description of the memory controller **12** is described with respect to hardware components, all of the functions described hereinafter may also be implemented in software, for execution by the microcontroller **64**.

The memory controller **12** comprises a current cache page address registers **66** which may be implement in the nature of a content addressable memory **66**. The function of the CAM **66** is to keep current PNOR cache page addresses and to update the CAM **66** when there is an access miss during either a read or write operation to the PNOR portion **52**. Each entry within the CAM **66** has three portions: a page address portion **66***a*, an index address portion **66***b*, and a status portion **66***c*. The discussion that follows with regard to the operation of the memory controller and the CAM memory **66** is with regard to the following example, although it should be understood that the invention is not limited to the following example. It is assumed that the address from the host device **20** is 32 bits, comprising of 21 most significant bits (bits **11-31**) and 11 least significant bits (bits (**0-10**). The 21 most significant bits comprises a page address, while the 11 least significant bits comprises an offset address. Each entry in the CAM memory **66** also comprises the page address portion **66***a* comprising of 21 bits, the index address portion **66***b* comprising of 9 bits, and the status portion comprising of 12 bits, which consist of 1 bit of valid (or not); 1 bit of dirty (or clean); 1 bit of static (or dynamic); 1 bit of host initiated cache coherence (or controller initiated); and 8 bits for last access time stamp. With 32 bits from the host device **20**, the host device can address 2^{32} Bytes or 1 GB amount of memory space. As will be discussed hereinafter, the memory controller **12** uses the index address portion of 9 bits from the CAM memory **66** along with the 11 bits from the offset address from the host device **20** to form a 20 bit address thereby enabling the addressing of 1 MB to the RAM **16**. Of course, these numbers are by way of example only and do not limit the present invention.

The memory controller **12** also comprises a Hit/Miss compare logic **68**. The Hit/Miss compare logic **68** receives the address signals from the address bus **22**, and the control signals from the control bus **32**. The Hit/Miss compare Logic **68** then sends the 21 bits of the page address from the 32 bits of address from the host device **20** to the CAM memory **66**. The CAM memory **66** compares those 21 bits of page address with page address **66***a* stored in each entry of the CAM memory **66**. If there is a HIT, i.e. the 21 bits of the page address from the host device **20** matches one of the entries in the CAM memory **66**, then the CAM memory **66** outputs the associated 9 bits of the index address **66***b*, to the MUX **70**. If there is a Miss, the Hit/Miss compare logic **68** generates a read miss signal or a write miss signal. The read miss signal and the write miss signals are supplied to a Micro Code Controller (MCC)/Error Code Correction (ECC) unit **72** as signals for the MCC/ECC unit **72** to perform data coherence. The signal supplied to the MCC/ECC unit **72** is either a Hit: which indicates that one of current page address stored in the

RAM memory **16** is the address from the host device **20** as supplied on the address bus **22**, or a Miss: which indicates that none of the current page address stored in the RAM memory **16** is the address from the host device **20** as supplied on the address bus **22**. Finally, the Hit/Miss compare logic **68** is also connected to the wait state signal **26**. The wait state signal **26** is generated when the memory controller **12** desires to inform the host device **20** that the memory controller **12** desires to hold the bus cycle operation. The wait state signal **26** is de-asserted to release the buses **22**/**24**/**32** to permit the host device **20** to resume operation. One example of a wait state signal **26** being asserted by the memory controller **12** is when there is a read/write miss and the memory controller **12** needs to retrieve the data from the address in the NAND memory **14** and to load it into the RAM memory **16**. During the time that the data is retrieved from the NAND memory **14** and loaded into the RAM memory **16**, the wait state signal **26** is asserted by the memory controller **12**.

The memory controller **12** also comprises a MCC/ECC unit **72**, which operates under the control of the microcontroller **64**. The MCC/ECC unit **72** monitors the read miss/write miss signals for cache data coherence, flush replacement, and paging operations. In addition, under the control of the microcontroller **64**, it operates the NAND memory **14** and provides for the defect management operation of the NAND memory **14**. Further, under the control of the microcontroller **64**, the MCC/ECC unit **72** provides DMA function to move data between NAND memory **14**, RAM memory **16**, and SRAM memory **46**. Finally, the MCC/ECC unit **72** performs error detection and correction on the data stored in the NAND memory **14**.

The memory controller **12** also comprises a cryptograph engine **90**, which provides for security and digital rights management. In addition, the memory controller **12** may have additional RAM memory **92** embedded therein, i.e. formed on the same integrated circuit die, to be used to augment the amount of RAM memory **16**. As previously indicated the RAM memory **16** may be a separate integrated circuit die in which case the RAM memory **92** embedded in the memory controller **12** augments the RAM memory **16**. However, if the RAM memory **16** and the memory controller **12** are integrated into the same die, then the RAM memory **16** and the RAM memory **92** may both be part of the same memory array.

The memory device **10** will now be described with respect to the various modes of operation. During power up, the Hit/Miss compare logic **68** generates the wait signal and asserts the wait state signal **26**. The memory controller **12** reads the configuration parameters from the non-volatile registers **60** and loads them to the volatile registers **46** (which may be a part of the SRAM **46**). The static pages, i.e. data from the NAND memory **14** which are statically mapped to the PNOR portion **52** will also be read from the NAND memory **14** and stored into the RAM memory **16**. This is done by the microcontroller **64** through the MCC/ECC **72** executing the FFS protocol to translate the address of the page from the NAND memory **14** and to generate the physical address and control signals to the NAND memory **14** to retrieve the data therefrom and to store them into the RAM memory **16**. During power up, the MCU **64** and the MCC/ECC **72** will also scan the NAND memory **14** to find the master index table. The master index table will be read and stored into the local SRAM memory **46**. The MCU **64** will check the data structure integrity of the master index table. The MCU **64** and the MCC/ECC **72** will also scan the NAND memory **14** to determine if rebuilding of the master index table is required. The MCU **64** and the MCC/ECC **72** also will bring two pages of data from the NAND memory **14** into the local SRAM memory **64**. The first two pages of data from the NAND memory **14**, called Vpage contains data for mapping the logic address of the host device **20** to the physical address of the NAND memory **14** with the capability to skip defective sectors in the NAND memory **14**. The FFS is then ready to accept mapping translation request. The Hit/Miss compare logic **68** then de-asserts the wait state signal **26**, i.e. releases the wait state signal **26**.

It should be noted that during power up, while the memory controller **12** is retrieving the static pages from the NAND memory **14** and storing them into the RAM memory **16**, and performing other overhead functions, such as updating the master index table of the NAND memory **14**, the memory device **10** is still available for use by the host device **20**. In particular, the NOR memory **44** can be accessed by the host device **20** even during power up, since the assertion of the wait state signal **26** affects only those operations directed to address requests to the PNOR portion **52** of the memory space.

NOR Memory Operation

In a NOR memory **44** read operation, the host device **20** sends an address signal on the address bus **22** which is within the NOR memory access portion **50** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. Because the address signals are in a space other than in the PNOR memory access portion **52**, the Hit/miss compare logic **68** is not activated, and the wait state signal **26** is not asserted. The address signals and the control signals are supplied to the NOR memory **44**, where the data from the address supplied is read. The data is then supplied along the data bus to the MUX **84** and out along the data bus **24** to the host device **20**, thereby completing the read cycle.

In a NOR memory **44** write or program operation, the host device **20** sends an address signal on the address bus **22** which is within the NOR memory access portion **50** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. Because the address signals are in a space other than in the PNOR memory access portion **52**, the Hit/miss compare logic **68** is not activated, and the wait state signal **26** is not asserted. The address signals and the control signals are supplied to the NOR memory **44**. The data and program commands to be written or programmed is sent along the data bus **24** from the host device **20** to the memory controller **12** and into the MUX **84**. From the MUX **84**, the data is then sent to the NOR memory **44**, where the data is programmed into the NOR memory **44** at the address supplied on the address bus **22**. The host device **20** can perform byte program operation allowing the NOR memory **44** to be programmed on a byte-by-byte basis. The write or program cycle is completed when the data is written into the NOR memory **44**.

In NOR memory **44** erase operation, such as sector erase, or block erase, the host device **20** sends an address signal on the address bus **22** which is within the NOR memory access portion **50** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. Because the address signals are in a space other than in the PNOR memory access portion **52**, the Hit/miss compare logic **68** is not activated, and the wait state signal **26** is riot asserted. The address signals and the control signals are supplied to the NOR memory **44**. The data signal representing the erase command protocol is sent along the data bus **24** from the host device **20** to the memory controller **12** and into the MUX **84**.

From the MUX **84**, the data is then sent to the NOR memory **44**, where the data is decoded by the NOR memory **44** and the erase operation is then executed. The erase cycle is completed when the NOR memory **44** completes the erase cycle.

PNOR Memory Operation—Read

In a PNOR memory read operation, the host device **20** sends an address signal on the address bus **22** which is within the PNOR memory access portion **52** of the memory space to the memory device **10**. There are two possibilities: Read Hit and Read Miss.

In the case of a Read Hit, the page address portion of the address signals supplied on the address bus **22** are received by the Hit/Miss compare logic **68**, and are compared to the addresses currently in the RAM memory **16**, as stored in the CAM **66**. If the page address supplied on the address bus **22** is within a page address stored in the CAM **66**, then there is a hit. The Hit/Miss logic **68** activates the MUX **70** such that the address and control signals are then directed to the RAM memory **16**, with the associated index address **66***b* from the CAM memory **66** concatenated with the offset address from the host device **20** to address the RAM memory **16**. Data read from that lower address from the RAM memory **16** are then sent to the MUX **80** where they are then supplied to the MUX **84** (the default state for the MUX **80**), which has been directed (not shown) by the Hit/Miss compare logic **68** to permit the data to be sent to the host device **20** along the data bus **24**, thereby completing the read cycle.

In the case of a Read Miss, there are a number of possibilities. First, is the possibility called Read Miss without cache flush. In the event the comparison of the page address portion of the address signals from the address bus **22** to the page address register **66***a* from the CAM **66** results in a miss, i.e. the page address on the address bus **22** is not within the addresses of pages stored in the RAM memory **16**, the Hit/Miss compare logic **68** then sends a read miss signal to the MCC/ECC unit **72** for the MCC/ECC unit **72** to initiate a read coherence cycle. In addition, the Hit/Miss compare logic **68** asserts a signal on the wait state signal **26**. The MCC/ECC unit **72** under the control of the MCU **64** executes an FFS operation to translate the address supplied by the host device **20** into a physical address in the NAND memory **14**. The MCC/ECC unit **72** then generates the appropriate address and control signals to the NAND memory **14**, and the appropriate address and control signals to the RAM memory **16**.

An entire page of data, including data from the address specified on the address bus **22** is read from the NAND memory **14** and is transferred through the MUX **80** and to the RAM memory **16**, where it is written into an entire page of locations in the RAM memory **16** specified by the MCC/ECC unit **72**, and is operated thereon by the MCC/ECC unit **72** to ensure the integrity of the data, through error correction checking and the like. The current page address registers of CAM **66** is then updated to add the address of the address page within the current read miss address. The Hit/miss compare logic **68** de-asserts the signal on the wait state signal **26**. In addition, the MCU **64** switches the MUX **80** to the default position. The Hit/Miss compare logic **68** sends the index address **66***b* to the MUX **70** where it is combined with the offset address portion from the address bus **22**, to address the RAM memory **16**. The data from that read operation on the RAM memory **16** is then supplied through the MUX **80** and through the MUX **84** to the data bus **24** to the host device **20**, thereby completing the cycle. Because the amount of data read from the NAND memory **14** is on a page basis, the entire page of data must be stored in the RAM memory **16**. This scenario of Read Miss without cache flush assumes that either an entire page of RAM memory **16** is available to store the data from the NAND memory **14**, or the location in the RAM memory **16** where an entire page of data is to be stored contains coherent data (same as the data in the NAND memory **14**), then the entire page of data read from the NAND memory **14** can be stored in a location in the RAM memory **16**. Cache flush means the writing of data from the RAM memory **16** to NAND memory **14**, thereby flushing the cache (RAM memory **16**) of the data coherence problem.

Another possible scenario of a Read Miss is called Read Miss with cache flush. In this scenario, an entire page of data from the NAND memory **14** cannot be stored in the RAM memory **16** without overwriting some data in the RAM memory **16** which is newer than the data in the NAND memory **14**. This creates a data coherence problem. Thus, a page of data in the RAM memory **16** must first be written into the NAND memory **14**, before the data from the NAND memory **14** in a different location can be read into the RAM memory **16**. The sequence of operations is as follows. The page address portion of the address signal from the address bus **22** from the host device **20** is compared to the page address signals **66***a* from the CAM **66** to determine if the address signal from the address bus **22** is within any of the current page addresses. This comparison results in a miss, causing the Hit/Miss compare logic **68** to send a read miss signal to the MCC/ECC unit **72** for the MCC/ECC unit **72** to initiate a read coherence cycle. In addition, the Hit/Miss compare logic **68** asserts a signal on the wait state signal **26**. The MCC/ECC unit **72** under the control of the MCU **64** determines that a page of data in the RAM memory **16** must first be written into the NAND memory **16** because there is a data coherence problem should the data from the NAND memory **14** be read into the RAM memory **16**. The MCU **64** executes an FFS operation to translate the address from the RAM memory **16** into the address in the NAND memory **14**.

An entire page of data is read from the RAM memory **16**, passed through the MUX **80** and supplied to the NAND memory **14**, where they are stored in the NAND memory **14**. Thereafter, the address from the host device **20** is converted by an FFS operation into a physical NAND address by MCU **64**. The MCC/ECC unit **72** then generates the appropriate address and control signals under the direction of MCU **64** to the NAND memory **14** and using the index address **66***b* from the CAM memory **66** and the control signals and the offset address portion from the MCC/ECC **72** to address the RAM memory **16**. An entire page of data read from the NAND memory **14** is then transferred from the NAND memory **14** through the MUX **80** and to the RAM memory **16**, where it is written into a page of locations in the RAM memory **16** specified by the MCC/ECC unit **72** and the index address **66***b*, and is operated thereon by the MCC/ECC unit **72** to ensure the integrity of the data, through error correction checking and the like. The current page address registers **66***a* of CAM **66** is then updated to add the page address which contains the current read miss address, along with it associated index address **66***b*. The Hit/miss compare logic. **68** de-asserts the signal on the wait state signal **26**. In addition, the MCU **64** switches the MUX **80** to the default position. The Hit/Miss compare logic **68** sends the index address **66***a* to the MUX **70** where they are combined with the offset address from the address bus **22** to initiate a read operation in the RAM memory **16**. The data is then read from the RAM memory **16** and supplied through the MUX **80** and through the MUX **84** to the data bus **24** to the host device **20**, thereby completing the Read cycle.

In each of the cases of Read Hit, Read Miss without cache flush, and Read Miss with cache flush, from the host device **20** point of view, the operation is no different than a read to a RAM device, with latency in the case of a Read Miss. The host device **20** does not have to deal with address translation and/or data coherence.

PNOR Memory Operation—Write

In a PNOR memory write operation, the host device **20** sends an address signal on the address bus **22** which is within the PNOR memory access portion **52** of the memory space to the memory device **10**, along with the data to be written into the RAM memory **16**. There are two possibilities: Write Hit and Write Miss.

In the case of a Write Hit, the page address portion of the address signals supplied on the address bus **22** are received by the Hit/Miss compare logic **68**, and are compared to the page addresses **66***a* in the CAM **66**, which reflect data currently stored in the RAM memory **16**. The page address supplied on the address bus **22** is within a page address stored in the CAM **66**. The Hit/Miss logic **68** activates the MUX **70** such that the address and control signals are then directed to the RAM memory **16**. The index address **66***b* from the CAM **66** and the offset address portion of the address signals from the address bus **22** are combined to produce an address signal used to access the RAM memory **16** through the MUX **70**. Data from the data bus **24** is supplied through the MUX **84** through the MUX **80** is supplied to the RAM memory **16**, where it is then written into the RAM memory **16**, thereby completing the Write Hit cycle.

It should be noted that the data in the RAM memory **16**, after the Write Hit operation will not be coherent with respect to the data from the same location in the NAND memory **14**. In fact, the data in the RAM memory **16** will be the most current one. To solve the problem of data coherency, there are two solutions.

First, the memory device **10** can automatically solve the problem of data coherence, on an as needed basis. As discussed previously, for example, in the case of a Read Miss with Cache Flush operation, data that is more current in the RAM memory **16** will be written back into the NAND memory **14** if the pages of data in the RAM memory **16** need to be replaced to store the newly called for page of data from the NAND memory **14**. As will be discussed hereinafter, the MCU **64** will also perform a cache flush on the data in the RAM memory **16** by writing the data back into the NAND memory **14** in a Write Miss with Cache Flush operation.

An alternative solution to the problem of data coherence is to perform data coherence under the control of the host device **20**. Thus, the host device **20** can issue a cache flush command causing the memory controller **12** to write data that is not coherent from the RAM memory **16** back into the NAND memory **14**. The advantage of this operation is that it can be done by the host device **20** at any time, including but not limited to critical events such as changing application, shutdown, or low power interruption received. However, because the memory controller **12** also can perform data coherence automatically, in the event the user of the host device **20** fails to perform the data coherence operation, such operation will also be performed as needed by the memory controller **12**.

In the case of a Write Miss, there are a number of possibilities. First, is the possibility called Write Miss without cache flush. In the event the comparison of the page address portion of the address signals from the address bus **22** to the page address signals **66***a* from the CAM **66** results in a miss, i.e. the address on the address bus **22** is not within the addresses of pages stored in the RAM memory **16**, the Hit/Miss compare logic **68** then sends a write miss signal to the MCC/ECC unit **72**. In addition, the Hit/Miss compare logic **68** asserts a signal on the wait state signal **26**. The MCC/ECC unit **72** determines if a new page of data from the NAND memory **14**, including the data at the address specified on the address bus **22** from the host device **20**, will store over either old coherent data, or a blank area of the RAM memory **16**. In that event, there is no need for the memory controller **12** to perform a write coherence cycle before transferring the data from the NAND memory **14** to the location in the RAM memory **16**. The MCC/ECC unit **72** under the control of the MCU **64** executes an FFS operation to translate the address supplied by the host device **20** into a physical address in the NAND memory **14**. The MCC/ECC unit **72** then generates the appropriate address and control signals to the NAND memory **14**, and the appropriate address and control signals to the RAM memory **16**.

An entire page of data, including data from the address specified on the address bus **22**, is read from the NAND memory **14** and is transferred through the MUX **80** and to the RAM memory **16**, where it is written into an entire page of locations in the RAM memory **16** specified by the MCC/ECC unit **72** and the index address **66***b*, and is operated thereon by the MCC/ECC unit **72** to ensure the integrity of the data, through Terror correction checking and the like. The current page address registers **66***a* of CAM **66** is then updated to add the address of the address page within the current write miss address and the associated index address **66***b* (the index address **66***b* being the upper 9 bits of the address in the RAM memory **16** where the page of data is stored). The Hit/miss compare logic **68** de-asserts the signal on the wait state signal **26**. In addition, the MCU switches the MUX **80** to the default position. The Hit/Miss compare logic **68** sends the index address **66***b* to the MUX **70** where they are combined with the offset address from the address **22**, to initiate a write operation in the RAM memory **16**. The data is then written into the RAM memory **16** from the host device **20** through the MUX **84** and through the MUX **80**, thereby completing the cycle. The data in the RAM memory **16** is now no longer coherent with the data at the same address in the NAND memory **14**. This coherence problem be solved by either the memory controller **12** initiating a write cache flush, automatically on an as needed basis, or by the host device **20** initiating a write cache flush, at any time, all as previously discussed.

Another possible scenario of a Write Miss is called Write Miss with cache flush. In this scenario, an entire page of data from the NAND memory **14** cannot be stored in the RAM memory **16** without overwriting some data in the RAM memory **16** which is newer than the data in the NAND memory **14**. This creates a data coherence problem. Thus, a page of data in the RAM memory **16** must first be written into the NAND memory **14**, before the data from the NAND memory **14** in a different location can be read into the RAM memory **16**. The sequence of operations is as follows. The page address portion of the signal from the address bus **22** from the host device **20** is compared to the page address signals **66***a* from the CAM **66** to determine if the address signal from the address bus **22** is within any of the current page addresses. This comparison results in a miss, causing the Hit/Miss compare logic **68** to send a write miss signal to the MCC/ECC unit **72** for the MCC/ECC unit **72** to initiate a write coherence cycle. In addition, the Hit/Miss compare logic **68** asserts a signal on the wait state signal **26**. The MCC/ECC unit **72** under the control of the MCU **64** determines that a page of data in the RAM memory **16** must first be written into the NAND memory **16** because there is a data coherence problem should the data from the NAND memory **14** be read into the RAM memory **16**. The MCU unit **64** executes an FFS operation to translate the address from the RAM memory **16** into the address in the NAND memory **14**.

An entire page of data is read from the RAM memory **16**, passed through the MUX **80** and supplied to the NAND memory **14**, where they are stored in the NAND memory **14**. Thereafter, the address from the host device **20** is converted by an FFS operation into a physical NAND address. The MCC/ECC unit **72** then generates the appropriate address and control signals to the NAND memory **14** using the physical NAND address from the FFS, and the index address and control signals to the RAM memory **16**. An entire page of data read from the NAND memory **14** is then transferred from the NAND memory **14** through the MUX **80** and to the RAM memory **16**, where it is written into a page of locations in the RAM memory **16** specified by the offset address from the MCC/ECC unit **72** and the index address from the index address register **66***b*, and is operated thereon by the MCC/ECC unit **72** to ensure the integrity of the data, through error correction checking and the like. The current page address registers of CAM **66** is then updated to add the page address **66***a* which contains the current read miss address, and the associated index address **66***b*. The Hit/miss compare logic **68** de-asserts the signal on the wait state signal **26**. In addition, the MCU switches the MUX **80** to the default position. The Hit/Miss compare logic **68** sends the index address **66***b* to the MUX **70** where they are combined with the offset address from the address bus **22** to form an address to write in the RAM memory **16**. The data is then written into the RAM memory **16** from the host device **20** to the data bus **24** through the MUX **84** and through he MUX **80**. Similar to the foregoing discussion for Write Miss without Cache Flush, the data in the RAM memory **16** is now more current and a data coherence problem is created, which can be solved by either the host device **20** initiating a cache flush, or the memory controller **12** initiating a cache flush operation.

In each of the cases of Write Hit, Write Miss without cache flush, and Write Miss with cache flush, from the host device **20** point of view, the operation is no different than a write to a RAM device, with latency in the case of a Write Miss. The host device **20** does not have to deal with address translation and/or data coherence.

To further reduce the latency time in the event of a Read Miss with cache flush or a Write Miss with cache flush, caused by the need to first perform a write operation to the NAND memory **14** from the RAM memory **16** to solve the data coherence problem, the following can be implemented. The page of data that is to be written into the NAND memory **14** is first written into the local SRAM **46** from the RAM memory **16**. This is a much faster operation than writing directly into the NAND memory **14**. Thereafter, the Read Miss with Cache Flush or Write Miss cache flush operation continues as if it were a Read Miss without cache flush or Write Miss without Cache Flush operation. After the Read Miss or Write Miss operation is completed, the data stored in the local SRAM **46** can be written into the NAND memory **14** in background operation when the memory device **10** is idle or access is limited to operation in the NOR memory access portion **50** or RAM memory access portion **54** or the configuration register access portion **56**.

It should be noted that in a PNOR operation, from the host device **20** point of view, the operation is no different than executing to a RAM memory, with the data being non-volatile, but without the host device **20** issuing NOR protocol commands, such as Sector or Block ERASE. However, it is also within the present invention that the memory device **10** can emulate NOR operation using RAM memory **16** and NAND memory **14**. In that event the memory space mapping for the NOR memory access portion **50** would extend to more than just mapping to the NOR memory **44**. The NOR memory access portion **50** can be mapped to a portion of the RAM memory **16**, with the RAM memory **16** mapped to the NAND memory **14** statically thereby presenting no latency problem during access. The data from the NAND memory **14** would be loaded into the RAM **16** on power up, and read/write to the NOR memory access portion **50** would be reading from or writing to the RAM memory **16**. The only other change would be for the memory controller **12** to be responsive to the NOR protocol commands. As previously discussed, when such NOR protocol commands are issued by the host device **20**, they are supplied as a sequence of unique data patterns. The data, supplied on the data bus **24** would be passed through the MUX **84** through the MUX **80**. Because the address supplied on the address bus indicates that the operation is to be in a NOR memory access portion **50** emulated by RAM memory **16**, the MUX **74** is switched permitting the MCU **64** to receive the data pattern. Once that data pattern is decoded as a NOR command, the MCU operates the NAND memory **14** with those NOR commands, if for example the command is erase. Of course, the RAM memory **16**, being volatile memory does not have to be "erased". Thus, the execution of the NOR protocol commands would result in a faster operation by a RAM memory **16** emulating NOR memory **44** than a true NOR memory **44** executing the NOR protocol commands. Further, the emulation need not emulate the full set of NOR protocol commands. Instead, the controller **12** can emulate a partial set of the NOR protocol commands. Therefore, as used herein, the term "NOR protocol commands" means one or more commands from the full set of NOR protocol commands, promulgated by e.g. Intel or AMD.

RAM Memory Operation

In a RAM memory **16** read operation, the host device **20** sends an address signal on the address bus **22** which is within the RAM memory access portion **54** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. Because the address signals are in the RAM memory access portion **54**, the Hit/miss compare logic **68** activates the MUX **70** to permit the address/control signals from the address bus **22** and control bus **32** to be supplied to the RAM memory **16**. However, the wait state signal **26** is not asserted. In addition, the address from the host device **20** is decoded and from an address signal which is supplied to the RAM memory **16** along with the control signal from the control bus **32**, where the data from the address supplied is read. The data is then supplied along the data bus to the MUX **80** and the MUX **84** and out along the data bus **24** to the host device **20**, thereby completing the read cycle.

In a RAM memory **16** write operation, the host device **20** sends an address signal on the address bus **22** which is within the RAM memory access portion **54** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. Because the address signals are in the RAM memory access portion **54**, the Hit/miss compare logic **68** activates the MUX **70** to permit the address/control signals from the address bus **22** and control bus **32** to be supplied to the RAM memory **16**. However, the wait state signal **26** is not asserted. In addition, the address from the host device **20** is decoded and form an address signal which is supplied to the RAM memory **16** along with the control signal from the control bus **32**, where the data from the data bus **24** is written into the RAM memory **16** at the address supplied.

From the perspective of a host device **20**, the operation of read or write in the RAM memory access portion is no different than accessing a RAM device with no latency.

Configuration Register Operation

In a Configuration Register operation, the host device **20** sends an address signal on the address bus **22** which is within the Configuration register access portion **56** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. The data is then written into the Non-Volatile Registers **60**.

NAND Memory Operation

In a NAND memory **14** read operation, the host device **20** sends an address signal on the address bus **22** which is within the Mass Storage Access section **58** or ATA memory access portion **58** of the memory space to the memory device **10**. In addition, appropriate control signals are sent by the host device **20** on the control bus **32** to the memory device **10**. Because the address signals are in a space other than in the PNOR memory access portion **52**, the Hit/miss compare logic **68** is not activated, and the wait state signal **26** is not asserted. The host device **20** follows the ATA protocol to read/write to task file registers **79** for an ATA read/write command. The task file registers **79** contain registers to store: command, status, cylinder, head, sector etc. The MCC/ECC unit **72** under the control of the MCU **64** operates the Flash File System which translates host logical address to NAND physical address, with the capability to avoid using defective NAND sectors. Reference is made to U.S. Pat. Nos. 6,427,186; 6,405,323; 6,141,251 and 5,982,665, whose disclosures are incorporated by reference in their entirety. Each logical address from the host device **20** has an entry in a table called Vpage. The contents of the entry points to the physical address where the logical address data is stored.

To read a page of data from the NAND memory **14**, the address signals and the control signals are supplied to the NAND memory **14**. The host device **20** follows the ATA protocol with the task file registers **79** storing the command and the logical address. Each sector size is 512 bytes. The host device **20** checks for the readiness of the memory **10** by reading the status register **79** which is in the task file register access portion **58** of the memory space. The host device **20** writes the “read” command into the command registers **79**, within the memory space **58**. The MCU **64** performs an FFS translation of the logical address to a physical address and the MCC/ECC unit **72** under the control of the MCU **64** reads the data from the NAND memory **14**, and transfers pages of data into the buffer **81**. After the entire page of data is stored in the Data Registers **81**, and is operated thereon by the MCC/ECC unit **72** to ensure the integrity of the data, through error correction checking and the like, the data is read out of the memory controller **12** along the data bus **24**.

An operation to write into the NAND memory **14** is similar to an operation to read from the NAND memory **14**. The host device **20** checks for the readiness of the memory **10** by reading the status register **79** which is in the task memory space **58** portion. The host device **20** writes one page of data into the Data register **81**, and then writes the “write” command into the command registers **79**, along with the logical address. Thereafter, the MCU **64** using the FFS converts the logical address to a physical address and the MCC/ECC unit **72** under the control of the MCU **64** writes the one page of data from the ATA buffer **81** into the NAND memory **14**.

The FFS updates a page of data by locating the physical address of the page to be updated. FFS finds an erased sector as a “buffer sector” or if there is no erased sector, it first performs an erase operation on a sector. FFS then reads the old data which has not been modified and programmed to the buffer sector. FFS then programs the updated page data. It then waits for the next request. If the next page is on the same erase sector, FFS continues the update operation. If the next page is outside of the transferring erase sector, the rest of the unmodified data will be copied to the buffer sector. The mapping table entry is changed to the buffer sector physical address. A new page update operation is then started.

Referring to FIG. **4** there is shown a second embodiment of a memory device **110**. The memory device **110** is similar to the memory device **10** shown in FIG. **1**. Thus, like parts with like numerals will be designated. The only difference between the memory device **110** and the memory device **10** is that in the memory device **100**, the second RAM bus **40** connects the RAM memory **100** directly to the host device **20**, rather then to the memory controller **12**. Thus, in the memory device **110**, the host device has direct access and control of the RAM memory **100**.

This difference between the embodiment of the memory device **10** and the embodiment of the memory device **110** is reflected in the memory mapping shown in FIG. **5**. Similar to the memory device **10**, the memory mapping for the memory device **110** comprises a NOR memory access portion **50** which is mapped to the NOR memory **44**, a PNOR memory access portion **52** which is mapped to the RAM memory **16** in the memory device **110**, which is then mapped to the NAND memory **14**, and a RAM memory access portion **54** mapped to the RAM memory **16**. However, with the RAM memory **100** being directly accessible by the host device **20** through the second RAM bus **40**, the memory mapping for the memory device **110** also includes another RAM memory access portion **55**, which maps directly to the RAM memory **100**. The memory device **110** then further comprises the configuration register access portion **56**, and finally an ATA memory access portion **58**, similar to that described for the memory device **10**.

With the memory controller **12** interfacing with the host device **20** and with the NAND memory **14**, the memory device **10** offers more protection than the memory devices of the prior art. In particular, the memory controller **12** can limit access to certain data stored in the NAND memory **14**, as in concerns relating to Digital Rights Management. Further the memory controller **12** can encrypt the data stored in the NAND memory **14** to protect sensitive data. Finally, the memory controller **12** can offer protection against accidental erasure of data in certain portion(s) of the NAND memory **14**. Finally with the program stored in NOR memory **62** the memory controller **12** is a self-starting device in that it does not require initial commands from the host device **20**.

There are many aspects of the present invention. First, the memory device **10** or **110** is a universal memory device. The memory device has a memory controller which has a first address bus for receiving a RAM address signals, a first data bus for receiving RAM data signals, and a first control bus for receiving RAM control signals. The memory controller has NOR memory embedded therein and further has a second address bus for interfacing with a volatile RAM memory, a second data bus for interfacing with the volatile RAM memory, and a second control bus for interfacing with the volatile RAM memory. The controller further has a third address/data bus for interfacing with a non-volatile NAND memory, and a third control bus for interfacing with non-volatile NAND memory. The memory device further having a RAM memory connected to said second address bus, said second data bus, and said second control bus. The memory device further having a non-volatile NAND memory connected to the third address/data bus and to the third control bus. The controller is responsive to address signals supplied on the first address bus whereby the NOR memory is responsive to a first address range supplied on the first address bus, whereby the RAM memory is responsive to a second address range supplied on the first address bus, and whereby the NAND memory is responsive to a third address range supplied on the first address bus.

In yet another aspect of the present invention, the memory device is a universal memory device, wherein the user can defined the memory space allocation. The memory device has a memory controller which has a first address bus for receiving a RAM address signals, a first data bus for receiving RAM data signals, and a first control bus for receiving RAM control signals. The memory controller has NOR memory embedded therein and further has a second address bus for interfacing with a volatile RAM memory, a second data bus for interfacing with the volatile RAM memory, and a second control bus for interfacing with the volatile RAM memory. The controller further has a third address/data bus for interfacing with a non-volatile NAND memory, and a third control bus for interfacing with non-volatile NAND memory. The memory device further having a RAM memory connected to said second address bus, said second data bus, and said second control bus. The memory device further having a non-volatile NAND memory connected to the third address/data bus and to the third control bus. The memory device is responsive to the user defined memory space allocation wherein in a first address range supplied on the first address bus, the memory device is responsive to NOR memory operation including being responsive to NOR protocol commands, and a second address range supplied on the first address bus, the memory device is responsive to RAM operation, and a third address range supplied on the address bus, the memory device is responsive to the NAND memory operating as an ATA disk drive device, wherein the first, second and third address ranges are all definable by the user

In yet another aspect of the present invention, memory device has a memory controller which has a first address bus for receiving a RAM address signals, a first data bus for receiving RAM data signals, and a first control bus for receiving RAM control signals. The memory controller further has a second address bus for interfacing with a volatile RAM memory, a second data bus for interfacing with the volatile RAM memory, and a second control bus for interfacing with the volatile RAM memory. The controller further has a third address/data bus for interfacing with a non-volatile NAND memory, and a third control bus for interfacing with non-volatile NAND memory. The memory device further having a RAM memory connected to said second address bus, said second data bus, and said second control bus. The memory device further having a non-volatile NAND memory connected to the third address/data bus and to the third control bus. The controller further having means to receive a first address on the first address bus and to map the first address to a second address in the non-volatile NAND memory, with the volatile RAM memory serving as cache for data to or from the second address in the non-volatile NAND memory, and means for maintaining data coherence between the data stored in the volatile RAM memory as cache and the data at the second address in the non-volatile NAND memory.

In another aspect of the present invention, the memory device has a memory controller which has a first address bus for receiving a NOR address signals, a first data bus for receiving NOR data signals and data protocol commands, and a first control bus for receiving NOR control signals. The memory controller further has a second address bus for interfacing with a volatile RAM memory, a second data bus for interfacing with the volatile RAM memory, and a second control bus for interfacing with the volatile RAM memory. The controller further has a third address/data bus for interfacing with a non-volatile NAND memory, and a third control bus for interfacing with non-volatile NAND memory. The memory device further having a RAM memory connected to said second address bus, said second data bus, and said second control bus. The memory device further having a non-volatile NAND memory connected to the third address/data bus and to the third control bus. The controller further operating the RAM memory to emulate the operation of a NOR memory device including NOR protocol commands.

One of the uses of the memory **10** or **110** of the present invention is in the PC system **300** shown in FIG. **6**. The memory device **10** or **110** can function in the following modes.

First, memory **10** or **110** can replace the DRAM **340**. Since the memory **10** or **110** has a RAM portion, it can replace the DRAM **340**. Furthermore, because the memory **10** or **110** also has a non-volatile portion, the memory **10** or **110** can store certain software in its NAND memory **14**, such that upon boot up of the PC **300**, the software can be immediately read from the NAND flash memory **14** through the controller **12** of the memory **10** or **110** and executed by the processor **314** without it being retrieved from the HDD **326**. In addition, certain data or program that is frequently used by a user, as monitored by the operating system can also be pre-fetched from the HDD **326** and stored in the NAND **14** or NOR memory **44** portion of the memory **10** or **110**, thereby saving time during operation as perceived by the particular user. Finally, the memory **10** or **100** can be used as a disk cache for the data/program from the HDD **326**.

Second, the memory **10** or **110** can replace the BIOS **320**. Because the memory **10** or **110** is operable in a NOR manner, the memory **10** or **110** can replace the BIOS **320** and can be used to store the start up code that the processor **314** requires to start the PC **300**. The interface to the Southbridge **318** from the BIOS **320** can be serial or parallel. In addition, the memory **10** or **110** can be partitioned into at least two parts: one part for storing the BIOS code and the other part to store code for the operating system. In that event, start up of the PC **300** may be more rapid since some of the operating code is in non-volatile memory portion of the memory **10** or **110** rather than being stored on HDD **326**. The controller **12** can provide security access to authorize one or the other portion. When operating in this mode, the memory **10** or **110** need not contain any RAM **16**. The memory **10** or **110** can be simply the controller **12** with a small amount of NOR memory **44** and a NAND Flash memory **14**, and need not contain any RAM **16** or be able to operate in a Pseudo NOR mode. Further, not all of the BIOS **320** instructions need to be stored in the NOR memory **44**. Some of the instructions for the BIOS **320** can be stored in the NOR memory **44** with the remainder stored in the NAND Flash memory **14**.

Third, the memory **10** or **110** can replace the BIOS **320** and with the bus **350** divided into two buses: a first bus **351**, parallel or SPI (serial) from the Southbridge **318** to the BIOS **320**, and a second bus **352**: an industry standard ATA bus from the Southbridge **318** to the BIOS **320**, as shown in FIG. **7A**. In this mode, which is a variation of the second mode described above, the memory **10** or **100** need not contain any RAM **16**. In addition to the functions of storage and retrieval of the BIOS instructions, because the memory **10** or **110** also has an ATA bus, it can be used as a "lite" HDD in applications where the PC system **300** is used as a thin client, not requiring an HDD **326**. Thus, the memory **10** or **110** can function as both a storage of the BIOS instructions as well as storage or operating system or user data in the NAND Flash memory **14**. Thus, as used herein, the bus **350** can mean any type of bus or group of buses, including but not limited to PCI, PCI express, USB, ATA etc.

Fourth, the memory **10** or **100** can replace the BIOS **320** and with the bus re-routed such that the memory **10** or **100** is interposed between the signal from the Southbridge **318** to the HDD **326** or to the USB port **327** as shown in FIG. **7**B. Because the memory **10** or **110** has a controller **12**, there are three modes it can operate. First, it can be totally transparent, i.e. as if the memory **10** or **110** is not present, with the communication on the bus **350** directed from the Southbridge **318** to the HDD **326** or the USB port **327**. Second, the memory **10** or **110** can "intelligently" listen to the signals representing command or data between the Southbridge **318** and the HDD **326** and "trap" or "capture" any such command or data. If the data requested by the Southbridge **318** is stored in the memory device **10** or **110**, the memory device **10** or **110** can respond thereto without the HDD **326** responding. Thus, performance is improved by the memory device **10** or **110** acting as a cache for the HDD **326**. It should be noted that this mode of operation does not require any special software driver. Third, the memory **10** or **110** can "trap" the command and re-transmit the command after analysis. Finally, with the PC **300** in an off mode, the MCU **12** and the memory device **10** or **110** can act as a host to the HDD **326** and control the operation thereof. This capability will be discussed in greater detail hereinafter. Here again, when operating in this mode, the memory **10** or **110** need not contain any RAM **16**. The memory **10** or **110** can be simply a small amount of NOR memory **44** and a NAND Flash memory **14**. Similar to the third mode of operation, the bus **350** that connects the Southbridge **318** to the BIOS **320** and to the Hard Drive **326** can comprise a group of buses such as: a parallel or SPI bus **351** for accessing the NOR memory **44** and an industry standard ATA bus **352** for accessing the NAND memory **14**. The NOR flash memory **44** can serve to store instructions for BIOS **320**, as previously discussed, when access to the BIOS **320** is along the parallel or SPI bus **351**. In addition, because the NAND Flash memory **14** is cheaper than NOR memory **44**, the NAND Flash memory **14** can be used to store the rest of the instructions for the BIOS **320** and retrieved into the MCU **12** and supplied along the parallel or SPI bus **351**. In addition, the NAND flash memory **14** can be used to store cache data from the Hard Disk Drive **326**, when the Southbridge **318** attempts to retrieve the data from the HDD **326** along the ATA bus **352**. A variation of the example shown in FIG. **7**B is shown in FIG. **7**C wherein the memory device **10** Or **110** is also connected to the Northbridge chip **316** through either a PCI bus, PCI express bus, or a USB bus.

Fifth, because the MCU **12** in the memory device **10** or **110** is a processor, it can be programmed to serve other functions, than the ones described heretofore. For example, the MCU **12** can be programmed such that the memory device **10** or **110** can function as an MP3 player or video play back with the songs/video stored in the NAND memories **14**. The program code necessary to operate the MCU **64** of the memory controller **12** can be stored in the NOR memory **62**. If the MCU **12** is not robust enough or it is desired to have dedicated hardware perform the MP3/video function, then either a dedicated DSP processor or a dedicated MP3 player processor can be integrated into the memory device **10** or **110**. Thus, with this feature, whether the PC **300** is on or not, the memory device **10** or **110** can play back the songs or video stored on the NAND memories **14**.

Sixth, with the memory device **10** or **110** having its MCU **12** programmed for MP3 or video playback or with the memory device **10** or **110** having a dedicated DSP processor for MP3 or video playback, even when the PC **300** is off or is in a hibernating mode, the memory device **10** or **110** can access additional audio/video data stored on the HDD **326**.

In addition to the features of the above mentioned sixth mode, in the event the PC **300** has an additional display, e.g. a smaller secondary display, with the PC **300** off or in a hibernating mode, the memory device **10** or **110** can retrieve audio-visual data stored on the HDD **326** and display them on either the primary display **332** or a secondary display (not shown). Again, in this mode of operation the only "active" component of the PC **300** that requires power would be the memory device **10** or **110**, the HDD **326** and the display **332** or the secondary display (not shown). Thus, with a smaller secondary display, which is "active" only when the memory device **10** or **110** is "on" when the processor **314** is in the off mode or in the hibernating mode, power savings is gained.

Finally, in a seventh mode, with the bus **350** also connected to external ports, such as USB port **327**, the memory device **10** or **110**, when the processor **314** is on, can act as a USB hub, or as a USB pass through device. However, when the processor **314** is off, the memory device **10** or **110** can act as the USB host, i.e. the memory device **10** or **110** controls and powers all devices connected to the USB port **327**. It should be noted that the USB bus is only just one example of the type of bus to which the present invention is directed. As previously discussed, the bus **350** can be any type of bus including but not limited to PCI, PCI express, ATA etc. Among the devices that can be connected to the USB port **327** include, card reader, that provides system **300** with file image back up to the HDD **326**; external USB storage device for additional storage or backup; and additional devices such as Bluetooth communication device. Thus, in this mode, it would be possible to "copy" a file from the HDD **326** without powering on the entire PC **300**.

What is claimed is:

1. A controller circuit comprising:

a first plurality of ports for connecting to a first plurality of buses for receiving and providing signals therefrom, and a second plurality of ports for connecting to a second plurality of buses for receiving and providing signals therefrom;

a third port for connecting to a memory;

said controller circuit operable in one of two modes: wherein in a first mode, said controller circuit functions as a pass through device to provide signals transparently to and from the plurality of first buses to the plurality of second buses; and wherein in a second mode, said controller circuit functions to monitor signals from one of the second plurality of buses to another of said second plurality of buses, in response to said signals requesting data from said controller circuit wherein said controller circuit analyzes said signals to determine if said data is in said memory.

2. A controller circuit comprising:

a first plurality of ports for connecting to a first plurality of buses for receiving and providing signals therefrom; and a second plurality of ports for connecting to a second plurality of buses for receiving and providing signals therefrom;

a third port for connecting to a memory;

said controller circuit operable in one of two modes: wherein in a first mode, said controller circuit functions as a pass through device to provide signals transparently to and from the plurality of first buses to the plurality of second buses; and wherein in a second mode, said controller circuit functions to trap signals from one of the second plurality of buses and analyzes said signal to determine whether to transmit said signal to another of said second plurality of buses, in response to said signals requesting data from said controller circuit, wherein said controller circuit analyzes said signals to determine if said data is in said memory.

3. The controller circuit of claim **1** wherein said memory is a non-volatile memory.

4. The controller circuit of claim **2** wherein said memory is a non-volatile memory.

5. A memory device comprising:

a first plurality of ports for connecting to a first plurality of buses for receiving and providing signals therefrom, and a second plurality of ports for connecting to a second plurality of buses for receiving and providing signals therefrom;

said memory device operable in one of two modes: wherein in a first mode, said memory device functions as a pass through device to provide said signals transparently to and from the plurality of first buses from and to the plurality of second buses; and wherein in a second mode, said device functions to monitor said signals from one of the second plurality of buses directed to one of said first plurality of buses, wherein said signals request data from said one of said first plurality of buses, and wherein said memory device serves to respond to said signals in the event said data requested is in said memory device.

6. A memory device comprising:

a first plurality of ports for connecting to a first plurality of buses for receiving and providing signals therefrom, and a second plurality of ports for connecting to a second plurality of buses for receiving and providing signals therefrom;

said memory device operable in one of two modes: wherein in a first mode, said memory device functions as a pass through device to provide said signals transparently to and from the plurality of first buses from and to the plurality of second buses; and wherein in a second mode, said device functions to trap said signals from one of the second plurality of buses directed to one of said first plurality of buses, wherein said signals request data from said first plurality of buses, and wherein said memory device serves to re-transmit said signals after an analysis of whether said data requested is in said memory device.

* * * * *