FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION

Field of the Invention

This invention relates to data encryption and decryption, and more particularly to an improved method and apparatus for using one level of encryption to establish a secure communication channel, then passing a decryption key over that channel for subsequent decryption. This invention includes a new method of scrambling bulk data. This invention is particularly useful for protecting bulk information intended for widespread distribution such as movies or music in CD or DVD formats.

Background of the Invention

The field of data encryption has been the subject of extensive scholarly investigation and has been the topic of many patents in the United States and other countries. For general reference, the background description in each of United States Patent Nos. 5,497,422 (Tysen et al., 5 March 1996) and 5,438,622 (Normile et al., 1 August 1995) discuss representative encryption schemes known in the art. Each of these patent applications are assigned to Apple Computer, Inc. These patents are incorporated herein by reference in their entirety.

A wide variety of information is sold to consumers in various forms. One major category of information is computer software. Another major category of information is music, often in the form of CDs or tape. Still another major category of information is movies, usually over cable or satellite television links but often in the form of analog tape or LaserDisc. There is a tension in distribution of any form of information because if consumers will buy it from a rightful owner, other consumers are likely to buy illegal copies made from legitimate originals.

Various copy protection schemes have been considered for use with various media. Scrambling of cable or satellite channels is common. A variety of anti-copying schemes are used in analog video tape. CDs or digital tape can be encoded with anti-copying codes.

Distribution of various information in digital form has troubled many content providers because making the information available potentially makes it quite simple for a user to make one or many illegal copies of that content. Forms of such content include movies, music, and data such as encyclopedic compilations. This issue has been widely discussed in relation to audio CDs, LaserDiscs and other formats.

In the personal computer environment, the protection of intellectual property has been of interest since the beginning of the industry. In computer software, a variety of special encoding or encryption schemes have been used. Some software requires a hardware key to be connected in some way to the computer system. Use of such systems frustrates casual copiers but often has some negative impact on legitimate users.

Due to the rapid growth of the industry and the technical difficulties associated with controlling information flow in an intrinsically open architecture, the industry players have more often than not written the problem off as intractable, at least in relevant time and cost frames. However, the problem remains. And as the convergence between entertainment and computing moves forward, driven by the evolution of hardware and software technologies, industry participants with different attitudes and requirements enter the discussion.

The problem is particularly acute with the advent of the DVD technology as a mass storage device in computers. DVD is a new, high density storage medium capable of storing about 4.5 through 18 gigabytes of information on a single 12 centimeter disc. Commercial products have already been announced before May 1996 for availability before December 1996.

The movie industry, with its high degree of sensitivity to intellectual property protection, is concerned that none of the new transmission modalities, including personal computers, enable free copying of their material. Other content providers have similar concerns. Some sort of copy protection scheme would encourage content providers, such as the movie industry, to distribute information such as movies in digital format.

The proposed protection scheme is intended to fall between a "screen door latch" (too weak) and a "Fort Knox" approach (too clumsy and expensive for mass-market products). Although it will be discussed here in the context of DVD, one skilled in the art will appreciate that this copy protection scheme can be used in many other situations or collections of elements.

Summary of the Invention

The invention provides a two-stage copy protection scheme. This is particularly useful where large quantities of data are to be encrypted and decrypted using an encryption key but that encryption key is to be carefully protected until the data is to be decrypted using an authorized retrieval system.

One stage of the retrieval system includes an encryption scheme to assure that the retrieval is made in an authorized system, and another stage of the retrieval system uses a stored encryption key to decode the data of interest. In one preferred implementation, the encryption key is used as a descrambling code.

To minimize the performance impact on the apparatus and not constrain use of system resources by low priority or low value data streams, the information flow can be broken into elements with a distinct hierarchy of bandwidth. For example, an MPEG stream (high bandwidth) may be merely scrambled, the scrambling control bits (much lower bandwidth) may be encoded, and only the MPEG-decode key information necessary to decode the scrambling control bits (very low bandwidth) is key encrypted.

The scrambling can be done in any of many ways, some of which are discussed in detail below. For example, the order of the data within a unit of data can be reordered in a controlled way to give a scrambled signal. Each unit of data, such as a 64 KB block, can be scrambled in a defined way, then a descriptor which characterizes that scrambling can be encrypted using a key and the encoded descriptor can be stored with the relevant block of data. A single key can be used to decrypt any scrambling descriptor and the descriptor can be changed for each unit of data, that is, each unit of data can be independently scrambled. With a key available, it is relatively straightforward to correctly reorder the scrambled data into the original, "clear text" format. With no key, if a sufficiently complex scrambling method has been chosen, it can be challenging to identify the correct key by trial and error, particularly since each data unit is scrambled in a different pattern. With the key, a moderately complex scrambling method will not have a significant effect on data reconstruction rate and thus becomes transparent to the user.

This copy protection becomes much more powerful if the key can be changed for different units of primary information, for example for each movie title.

Storage and access to this key raises an interesting challenge, but this can be managed very conveniently by using a separate encryption mode to secure the key and provide it in a coordinated fashion with the program of interest. One way to do this is to store the key in a secure manner on the same storage medium as the scrambled information. The mechanism of this separate storage mode can be set at a desired level of complexity. One preferred mode is to make this key inaccessible by typical access operations, but readily accessible through special operations. Specifically, in just one preferred embodiment, the key may be stored at a location which is inaccessible to a host computer which can only access a logical block address, but readily accessible to a drive control unit, which may be designed to access a specific physical address, preferably not a logical block address. This access capability can be designed into the drive control unit, and the relevant key can be stored at the corresponding location when the media is prepared.

Subsequent manipulation of the key can be under close security. Since the key need be extracted only once, taking even several seconds to extract and/or transfer the key will not have a significant impact on the user.

In one preferred embodiment, a public/private key pair is stored in a disk drive mechanism and a second public/private key pair is stored in a decryption/decode unit such as an MPEG2 decoder. The key pairs are used to establish a secure channel of communication between the disk drive and the decoder and, once the channel is secure, a message can be read safely from the storage medium into the decoder even if the data path for the channel between these elements is unsecure. This message is the information content or message protected using the high-level security scheme, but is itself the key for the low-level security scheme. Passing this encrypted key over a secure channel makes it extremely difficult to intercept the key and use it for improper purposes.

This inhibits casual copying by setting up the system so that the data flow path between a source, such as a DVD-ROM drive, and a destination, such as an MPEG decoder carries only scrambled information and decryption to clear text occurs only in an isolated portion of the system, preferably within a special descrambler/decoder unit. The scheme cannot be defeated except by system patches, and a new patch is required for each title defeated, that is for each new title encryption key.

Scrambling and encrypting the primary information means that a read of the media by a system that does not implement correct decoding will give unintelligible results. Only the application software, with a little help from the operating system, can allow correct decoding of the primary information, as in correct decoding and display of a movie.

Distributing the copy protection elements balances the economic and processing power burden so that no single part of the overall system bears all the cost and effort of protecting the valuable information. Modifying the media format to carry scrambled data and modifying the drive to take advantage of its closed sub-system status balances these costs.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**