(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 194 839**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 86301704.2

(22) Date of filing: 10.03.86

(51) Int.Cl.⁴: G 07 F 7/10

(30) Priority: 08.03.85 JP 46012/85

(43) Date of publication of application:
17.09.86 Bulletin 86/38

(84) Designated Contracting States:
DE FR GB

(71) Applicant: Kabushiki Kaisha Toshiba
72, Horikawa-cho Saiwai-ku
Kawasaki-shi Kanagawa-ken 210(JP)

(72) Inventor: Kamitake, Takashi c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura 1-chome
Minato-ku Tokyo 105(JP)

(72) Inventor: Mizutani, Hiroyuki c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura 1-chome
Minato-ku Tokyo 105(JP)

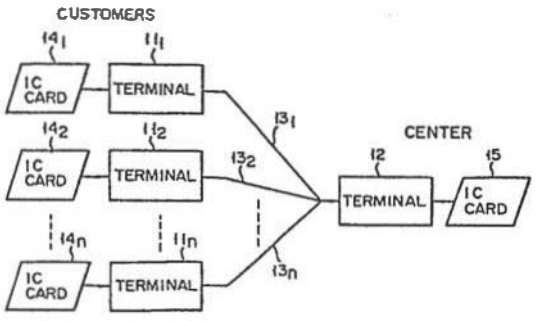
(72) Inventor: Kawamura, Shin-ichi c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura 1-chome
Minato-ku Tokyo 105(JP)

(74) Representative: Freed, Arthur Woolf et al,
MARKS & CLERK 57-60 Lincoln's Inn Fields
London WC2A 3LS(GB)

(54) Communications network using IC cards.

(57) A communication network has a plurality of customer terminals (11_1 - 11_n) and a single center terminal (12) which are coupled through communication lines (13_1 - 13_n). A large scale integrated circuit (IC card 14_1 - 14_n; 15) is operatively coupled to each terminal. The integrated circuit device has enciphering and deciphering functions and has a recording device (33). When a transaction request message is sent from one customer terminal to the center, the transaction request message is enciphered by the integrated circuit device, and the enciphered message is sent to the center. In order to increase the transaction verification capability, the transmission message is recorded, in association with encryption of the transmission message, in an area of the recording device which can be accessed from outside only for readout. In order to further improve the transaction verification capability, the response message is enciphered by the integrated circuit device in the center. The enciphered response message is deciphered by the integrated circuit device in the customer terminal. The response message is recorded in the area of the recording device such that the encrypted message and decrypted message can be distinguished from each other.

FIG. 1



EP 0 194 839 A2

Communications network using IC cards

The present invention relates to a communications network and, more particularly, to a communications network that enables transactions based on encrypted messages between terminals.

Recently, with developments in electronic technology, there have been innovations in communications network systems such as home banking and home shopping, and office banking systems. A vital concern regarding communications network systems for handling financial transactions is guaranteeing secrecy and security for these transactions. It is necessary to increase the verifiability of a transactor's identity or a message which is transmitted and received between transactors through the communications network.

The classical types of irregularities that can occur in the transmission of transactions or messages are as follows:

(1) False reports: A sender reports not sending to the receiver although a transmission was in fact made, or the sender reports sending although no transmission was made.

(2) Forgery of documents: A receiver rewrites a communication message that has been recorded on the receiving side, or forges a communication message.

These irregularities make embezzlement possible.

In a prior art system, in order to prevent such irregularities, an enciphering program such as DES (Data Encryption Standard) is stored in each network terminal to prevent the forging of communication messages. This means that an enciphering/deciphering circuit is provided in each terminal and that a sender, using his own key, enciphers a message according to this enciphering program. The enciphered message is transmitted to a receiver terminal through a communications network. On the receiver side, the received enciphered message is deciphered in the deciphering circuit using a key word which is stored in a key memory and is peculiar to the sender and then recorded. Accordingly, assuming that the key word stored in the key memory on the receiver side has not been leaked to the outside, and that the receiver has not forged the message, there is no one other than the sender who knows the key word who can make the enciphered message. Accordingly, the verifiability of the enciphered message stored on the receiver side is very high. Therefore, a digital signature can be made on the communication document. However, when the receiver changes his terminal operation mode from the decryption mode to the encryption mode, he can make an enciphered message using the sender's key word. Therefore, in a communciation network system based on an encryption/decryption scheme, irregularities between the sender and the receiver cannot be perfectly prevented, thus failing to guarantee the security of transactions.

European Patent Application Serial No. 85 30 3817,2 filed on May 30, 1985; entitled "COMMUNICATIONS NETWORK USING AN ENCIPHERING AND DECIPHERING DEVICE"; and assigned to the same assignee as this application discloses a communication network with LSI devices, such as IC cards, for enciphering/deciphering messages using a plurality of key words.

It is an object of the present invention to provide a communications network for performing communications

between terminals using enciphered messages, which guarantees transaction security.

It is another object of the present invention to provide a communications network system for performing communications between terminals using enciphered messages which enables a safe digital signature.

In a communications network system according to the present invention, first and second communication terminals are coupled via a communications network. First and second integrated circuit devices having a semiconductor large scale integrated circuit sealed therein are operatively coupled to the first and second terminals, respectively. The first IC device has at least a function for enciphering a first kind of messages input from the first terminal. The second IC device has at least a function for deciphering an enciphered message input from the second terminal. The first kind of messages enciphered by the first IC device is sent from the first terminal to the second terminal via the communications network.

According to the present invention, the first IC device has recording means. Together with encryption of the first kind of messages input from the first terminal, the first IC device is arranged to automatically record the first kind of messages (to be sent to the second terminal) in an area of the recording means, the area being accessible from outside of the IC device only for readout.

Furthermore, according to the present invention, the second IC device has a function for enciphering a second kind of messages (to be sent to the first terminal) input from the second terminal in response to the first kind of messages. The first IC device has a function for deciphering the second kind of messages sent from the second terminal to the first terminal and then input to the IC device. Together with decryption of the enciphered message the first IC device is

arranged to automatically record the second kind of messages in the area of the recording means that is accessible from outside only for readout.

In the first IC device, the first and second kinds of messages are recorded in the area of the recording means in such a way that the distinction between the first kind of messages to be enciphered and the second kind of messages which has been deciphered can be made.

This invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a schematic diagram of a communication system to which the present invention is applied;

Fig. 2 is a block diagram of terminals in Fig. 1;

Fig. 3 is a block diagram of IC cards used in the system in Fig. 1;

Fig. 4 is a diagram for explaining memory areas of a data memory in the IC card of Fig. 3;

Fig. 5 is a table for explaining access enable conditions of the memory areas;

Fig. 6 shows an access enable condition table of the data memory;

Fig. 7 is a format of a message applied to the IC card from the terminal;

Fig. 8 is a flow chart for explaining a communication transaction according to a first embodiment of the present invention;

Fig. 9 is a flow chart for explaining a communication transaction according to a second embodiment of the present invention;

Fig. 10 is a block diagram of a terminal suitable for detecting communications network failures;

Figs. 11 and 12 are diagrams for explaining recording methods for recording a transaction request message which is to be enciphered and a response message which has been deciphered in a data memory area in a distinguishable manner;

DOCKET ALARM

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.