United States Patent

Wolfe

[54] **VOICE CONFERENCE SYSTEM**

[72] Inventor: Fred G. Wolfe, Malvern, Pa.

[73] Assignee: Burroughs Corporation, Detroit, Mich.

[22] Filed: Feb. 26, 1970

[21] Appl. No.: 14,771

Related U.S. Application Data

[63] Continuation of Ser. No. 625,067, March 22, 1967, abandoned.

[52] **U.S. Cl.**..179/1.5 R, 179/1 CN
[51] **Int. Cl.**..H04m 3/16
[58] **Field of Search**..........................179/1.5, 1, 1.5 R, 1 CN

[56]   **References Cited**

UNITED STATES PATENTS

3,302,182	1/1967	Lynch et al.	340/172.5
2,437,707	3/1948	Pierce	179/1.5
2,449,467	9/1948	Goodall	179/1.5
2,453,461	11/1948	Shelleng	179/1.5
2,950,348	8/1960	Mayer et al.	179/1.5
3,071,649	1/1963	Goodall	179/1.5
3,384,717	5/1968	Coston	179/18

Primary Examiner—Benjamin A. Borchelt
Assistant Examiner—H. A. Birmiel
Attorney—Carl Fissell, Jr.

[57]   **ABSTRACT**

The present application discloses a voice conference system which may be utilized to provide virtual cut-through (VCT) service when used in conjunction with a modular data processor in a store and forward message switching system. The virtual cut-through service so provided allows the transmission of continuous traffic as well as digital voice communications. This feature coupled with other novel characteristics of the system make it possible to implement an extremely effective secure voice conference service.
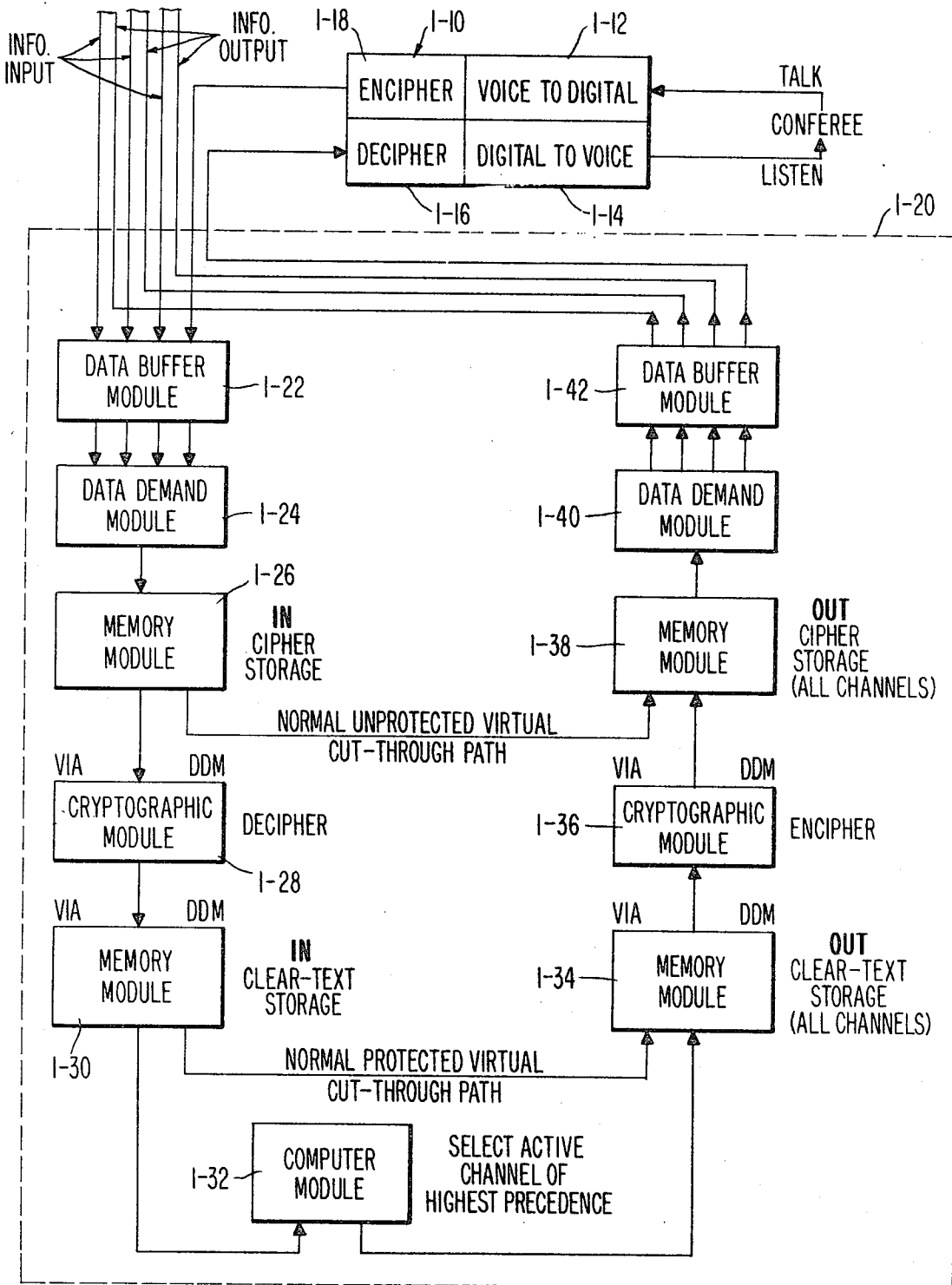
6 Claims, 4 Drawing Figures

INFO. INPUT

INFO. OUTPUT

I-18	I-10	I-12
ENCIPHER	VOICE TO DIGITAL	
DECIPHER	DIGITAL TO VOICE	
I-16	I-14	

TALK

CONFEREE

LISTEN

I-20

DATA BUFFER MODULE — I-22

DATA DEMAND MODULE — I-24

I-26

MEMORY MODULE

IN CIPHER STORAGE

NORMAL UNPROTECTED VIRTUAL CUT-THROUGH PATH

VIA   DDM

CRYPTOGRAPHIC MODULE   DECIPHER

I-28

VIA   DDM

MEMORY MODULE

IN CLEAR-TEXT STORAGE

I-30

NORMAL PROTECTED VIRTUAL CUT-THROUGH PATH

I-32 — COMPUTER MODULE

SELECT ACTIVE CHANNEL OF HIGHEST PRECEDENCE

I-42 — DATA BUFFER MODULE

DATA DEMAND MODULE

I-40

I-38 — MEMORY MODULE

OUT CIPHER STORAGE (ALL CHANNELS)

VIA   DDM

I-36 — CRYPTOGRAPHIC MODULE   ENCIPHER

VIA   DDM

I-34 — MEMORY MODULE

OUT CLEAR-TEXT STORAGE (ALL CHANNELS)

Fig. I

INVENTOR.
FRED G. WOLFF
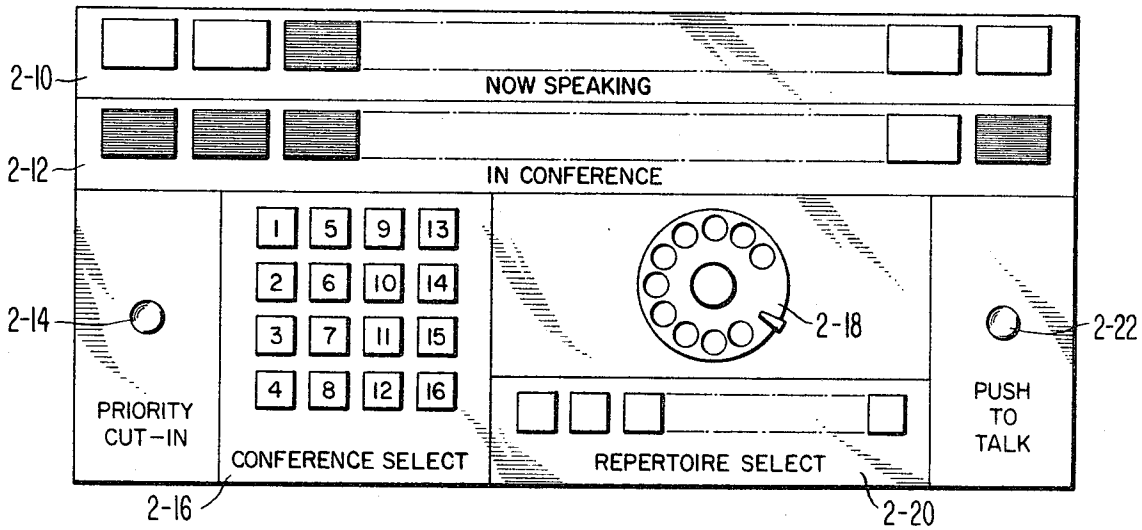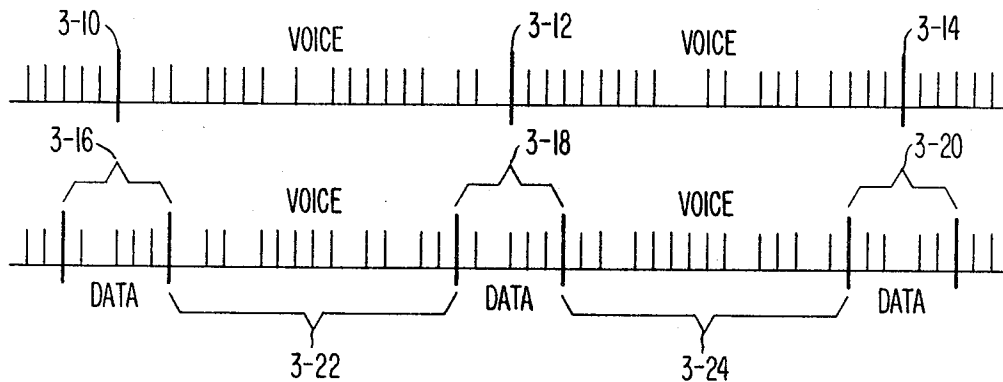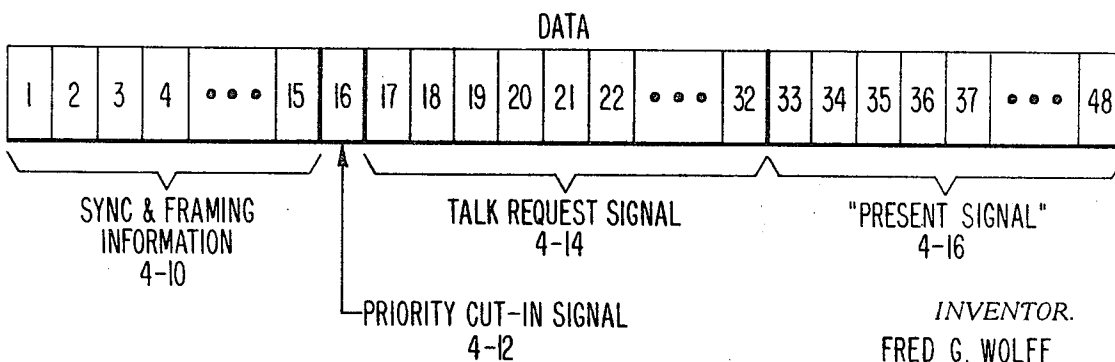BY Edward J. Feeney Jr.
ATTORNEY

Fig.2

Fig.3

Fig.4

INVENTOR.
FRED G. WOLFF

BY *Edward J. Feeney Jr.*

ATTORNEY

1

VOICE CONFERENCE SYSTEM

CROSS REFERENCE TO RELATED U.S. PATENT

This application is a continuation of an earlier application filed Mar. 22, 1967, Ser. No. 625,067 and now abandoned.

The content of the related patent entitled "A Store and Forward Message Switching System" by J.T. Lynch et al., U.S. Pat. No. 3,302,182, assigned to the present assignee, is to be included as part of this disclosure, since it is in such a system that the present invention will find a contemplated use.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the transmission and reception of continuous message traffic using a modular data processor as an automatic secure message switching center. In addition, the present invention discloses a means of providing the transmission of continuous traffic as well as digital voice communications.

For many applications, it is desirable to provide the equivalent of circuit-switching service in a message-switching center. One of these applications is the transmission of continuous traffic or very long messages; another, the transmission of voice communications.

2. Description of the Prior Art

Previous switching centers have been capable of continuous traffic or very long messages. However, in most cases, these systems required continuous supervision of the traffic during these long periods of transmission.

Another disadvantage of previous systems was that traffic did not arrive in the exact order in which it was transmitted, without interspersed messages from other sources.

In addition, because the same system components had to act upon each incoming message, and further because these components presented a fixed interface to all incoming messages, the use of special codes in a message or the requirement by a message of a special procedure was usually prohibited, since they were normally incompatible with the fixed switching center requirements and hence were not permitted.

Further, in those systems where voice communication was possible the element of immediacy ideally required was not always preserved.

BRIEF SUMMARY OF THE INVENTION

A system is provided for giving a modular data processinG system the facility for providing virtual cut-through (VCT) service which allows the transmission of continuous traffic as well as digital voice communications. The term Virtual Cut-Through refers to the ability of the system to receive the message and pass it through the system for transmission practically simultaneously. That is, it is accomplished as if the incoming circuit were actually switched to the outgoing circuit as is done in a circuit switching system. For example, in a telephone switching exchange the incoming call circuit is physically switched to the selected outgoing lines. This of course, would be actual cut through. In the present system this is accomplished without circuit switching. Rather it is accomplished by providing a path through the system between input and output lines virtually directly. It is done without any inspection of the incoming data whatsoever. This lack of inspection of the incoming data simulates still closer, the operation in a circuit switching system.

In the related U.S. Pat. No. 3,302,182, issued to the present assignee, entitled "A Store and Forward Message Switching System Utilizing a Modular Data Processing," By John T. Lynch and Fred G. Wolff, a rather different concept is described. As it's title implies, the incoming messages are received, stored and later forwarded out of the system. In the present system this store and forward feature is bypassed to accomplish a virtual cut-through the system by the message. Although a modular system is shown and described, however, it is not a specific requirement for the operation or practice of the presently proposed system. This, of course, does not

2

means that a data processing system is not necessary, it merely means that a modular system is not required. In a non-modular system, the conference is set up merely by connecting the conferees to the input and output buffer means of the data processing system. The advantages of using a modular system for a store and forward message switching system is set forth in the related application of Lynch et al. previously cited. However, as noted therein, switching centers are possible using data processing systems which are not modular. Thus, any switching center may utilize the present scheme provided it is one in which incoming and outgoing data are buffered before and after processing. Further, although a Cryptographic Module (CPM) is illustrated in the present embodiment, such a specific module is not required. In the absence of the cryptographic module secure traffic can be handled as described for unprotected traffic by the use of conventional cryptographic equipment. In the present system the virtual cut-through is accomplished by transferring all incoming data directly to the proper outgoing channel(s) without inspection of the data. Where protected channels are used this transfer is done after deciphering and before enciphering. Thus, different cryptographic techniques can be used on different channels.

A plurality of the individual modules from a Modular Data Processing system such as have been previously described in the U.S. Pat. No. 3,302,182 are utilized in a unique configuration. Thus a plurality of Data Buffer Modules (DBM) are utilized in conjunction with a plurality of Data Demand Modules (DDM) to provide a normal unprotected virtual cut-through path of communications through a plurality of Memory Modules. (MM)

When a normal protected (secured) virtual cut-through path is needed, an additional plurality of Cryptographic Modules together with a plurality of Memory Modules used in association with a Computer Module (CM) are required. Among the advantages of this configuration are:

1. The switching center is relieved of continuous supervision of traffic during long transmission periods;
2. Traffic arrives in the exact order in which it was transmitted, without interspersed messages from other sources;
3. Special codes and procedures, not compatible with normal switching center requirements, are permissible;
4. Generation of headers, etc., is not necessary;
5. The element of immediacy is preserved (for voice communication).

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features will become increasingly apparent when the following specification is considered in conjunction with the accompanying drawings. In the drawings:

FIG. 1 illustrates a block diagram showing the data flow for Virtual Cut-Through (VCT) over both protected and unprotected channels;

FIG. 2 shows an improved subscriber set configuration in a suggested embodiment;

FIG. 3 provides a digital coding scheme for use with the present system;

FIG. 4 illustrates a 48 bit data word showing the various signals and the framing information.

In a message switching center, it is not practical (nor desirable) actually to use circuit-switching techniques for the purpose of connecting the input message lines to the output message lines. Virtual cut-through can, however, be effected by transferring all incoming data directly to the proper outgoing channel(s), without inspection of the data. Where protected channels are used, this transfer is done after deciphering and before enciphering (in clear text). Thus, different cryptographic techniques can be used in different links. A Cryptographic Processor Module may be used just as in normal message-switching service. FIG. 1 illustrates the data flow for Virtual Cut-Through (VCT) over both protected and unprotected channels.

Once a VCT connection has been acquired, any kind of data, including digital voice, can be transmitted. Present secure voice transmission methods do not allow the superposition of two or more voices. Thus it is necessary to permit only one conferee to talk at a time. The controls that would be required for Secure Voice Conference Service are normally difficult to implement, partly because of their complexity. However, with a switching center, such as that disclosed in U.S. Pat. No. 3,302,182 available, the necessary control facility can be easily programmed into the switching center's processor. To prevent superposition of voices, a simple priority scheme is used, each participant automatically excluding those "below" him while he is talking. The assignment of conference precedence is made by the originator in the sequencing of routing indicators when setting up the call or by other procedural methods.

FIG. 1 shows the flow of information in and out of the switching center. Encrypted digital voice channels are independently received via the Data Buffer and Data Demand Modules, deciphered, and stored in memory. The Computer Module examines the various incoming channels and selects the one channel which will be transmitted to all conferees.

The actual methods of selection of the voice to be transmitted depends on the type of voice-encoding device used by the conferees. In its simplest form the incoming channel of highest (predetermined) precedence showing audio activity is selected for transmission. (A more complex scheme is also described below.) In any event, the data stored in the section of memory assigned to the selected channel is transferred to the appropriate memory section for independent re-enciphering and transmission to all conferees.

Any type of digital voice communication can be used provided, of course, that communication channels of sufficient bandwidth are available between each participant and the switching center. The voice-to-digital and digital-to-voice converters of all participants must be compatible; but cryptographic equipment used by subscribers may be of any type provided corresponding equipment is provided at the switching center. For example, if a Cryptographic Processor Module is included in the system, it can be shared by all links at the switching center provided their respective signalling speeds are the same.

To illustrate the additional capabilities of an automated secure message switching center when it is provided with a more sophisticated secure voice conference service, an improved subscriber set utilizing a digital coding scheme is shown in FIGS. 2,3 and 4. At regular intervals the digital voice stream is interrupted and a 48-bit data word inserted. This short interruption is not harmful to the voice quality. The data word contains a 15-bit sync marker code to identify it as a data word. In order to preclude the accidental interpretation of voice as data should this 15-bit sequence be generated by the voice equipment, the voice-generated data stream is continuously monitored, and should any sequence occur, one of its bits is arbitrarily inverted. This again, is not harmful to the voice quality. The 16 bit is a priority cut-in signal. Bits 17–32 are talk request signals for up to 16 conferees, and bits 33–48 are used to indicate the presence of the 16 conferees.

Data words sent by the subscriber to the switching center are utilized as follows. The voice to be transmitted is selected on the basis of bits 16 to 32. If bit positions 17 to 32 are assigned to subscribers in the order of predetermined precedence, the highest binary value (bit position 16 is considered high order; 32 low order) indicates the proper selection.

The data word is sent by each subscriber to the switching center. The data word to be sent by the switching center to each subscriber is generated in the following manner. The first 15 bits are, of course, the sync marker. Bits 16 through 32 are copied from the corresponding bits of the selected incoming channel. Bits 33 through 48 of all input channels are superimposed to produce the corresponding output bits.

At the subscriber set, the incoming data word is used to indicate visually those conferees present (bits 33 to 48), as well as the individual presently speaking (bits 17 to 32).

Some of the unused combinations of data bits are assigned to control functions, such as initiation and termination of calls. Such unused data bits are those bits available to each subscriber after his identification and speaking bits have been decided. Thus, each subscriber requires only one of the 16 bits (33 to 48) for indicating that he is present. Similarly, he requires only one bit (of bits 17 – 32) to shown that he is presently speaking. The remaining bits are available for other purposes.

Referring in particular to FIG. 1, there is illustrated in block form the subscriber set 1–10. In this set there is included a voice to digital converter 1–12, which receives the voice of the particular conferee and converts it to a corresponding binary digital representation. This digitally represented voice signal is then coupled to the enciphering means 1–18, where it is encoded in a predetermined manner. From there it is connected to the modular processing system as an input line to the Data Buffer Module 1–22. A number of other input information lines are also shown entering the Data Buffer Module 1–22. Such lines may be assumed to be connecting other subscriber sets similar to the set 1–10 to the modular processing system.

The Data Buffer Module may be of the type disclosed and described in the previously noted U.S. Pat. No. 3,302,182.

As its name implies, the enciphered information data is buffered into the system by this module. Next, the Data Demand Module 1–24 scans the respective lines of the Buffer Module 1–22 and transfers the selected information into the Memory Module 1–26.

From the stored contents of the Memory Module, the information may take one of two paths dependent upon whether the information is protected or unprotected. In this context, the words protected and unprotected mean secured and unsecured respectively. Thus classified messages would travel the protected or secured path while unclassified information would be passed along the unprotected or unsecured path.

In the case of a normal unprotected message, the virtual cut-through path would be directly to the Memory Module 1–38, from which it would pass through the Data Demand Module 1–40 and the Data Buffer Module 1–42 to information output lines. In the illustrated version, one set of output lines would be connected to the Digital to Voice Converter 1–14 for transfer to the Conferee.

A somewhat longer path is used for a protected message. In this case, the protected message leaves the Memory Module 1–26 and travels to the Cryptographic Module 1–28.

Although this path is shown as a direct line between the Memory Module and the Cryptographic Module, it should be noted that this is merely done for the sake of simplicity. Actually, the path is through the Data Demand Module 1–24 and this is noted on the drawing as via DDM.

From the Cryptographic Module 1–28, the protected path again travels via the Data Demand Module 1–24 prior to the storage of the protected message in clear text in the Memory Module 1–30. The protected message was, of course, deciphered in the Cryptographic Module prior to its transfer to the Memory Module 1–30.

From the Memory Module, the path of a normal protected virtual cut-through message travels to the Memory Module 1–34 for ultimate transfer out of the system. The protected message to be so transferred is selected by the Computer Module 1–32. This selection is based upon the degree of precedence and the Computer module 1–32 selects the active channel of the highest precedence in the Memory Module 1–34 to accomodate the transfer.

The clear text of the message of the selected channel passes into the Cryptographic Module 1–36. Here again this transfer is via a Data Demand Modules 1–40. The Cryptographic Module 1–38 enciphers the clear text of the message and then transfers it to the Memory Module 1–38 again via the Data Demand Module 1–40.

5

From the Memory Module 1–38 the path of a normal protected virtual cut-through is the same as the previously described path of a normal unprotected VCT. Thus the message passes to the subscriber set 1–10 and hence to the conferee.

In FIG. 2, a suggested embodiment of the subscriber is illustrated. For example, the conferee selects a plurality of individuals upon the pushbuttons of his conference selection means 2–16 and/or via the telephone-like dial 2–18, or similar signaling means. These are the particular parties whose presence he desires at the conference. Those persons at the conference are noted by the "in conference" lights 2–12, while the person speaking at the moment is noted by the illumination of a "now speaking" light 2–10. In addition a set of various predetermined conference groups are available to the speaker by the repertoire selection means 2–20.

Finally, the "push-to-talk" means 2–22 provides its noted function as does the "priority cut-in" means 2–14. It might be noted that the conference initiator can decide the individual priorities of the various conferees.

In FIG. 3, there is shown the digitally represented waveforms of a voice transmission. This is illustrated in the upper portion of the figure. At regular intervals 3–10,3–12,3–14 in the transmission a 48-bit data word is inserted. This is represented in greater detail in the lower portion of the figure wherein the data segments 3–16, 3–18, 3–20 of the transmission are shown inserted between the voice segments 3–22 and 3–24. It has been previously mentioned that these 48-bit data insertions are sufficiently short as not to appreciably affect the quality of the voice transmission.

Finally, FIG. 4 identifies the 48 bits of the data word. Bits 1–15 include the sync and framing information 4–10, bit 16 determines the priority cut-in signal 4–12, bits 17 to 32 provide the talk-request signal 4–14 and bits 33 to 48 indicate those present by the present signal 4–16.

While there has been shown and described a particular embodiment of the present invention, it is obvious that many modifications are possible which are within the scope of the present concept. It is, therefore, the applicant's intention to be bound only by the scope of the following claims.

6

I claim:

1. A secure voice conference system comprising a switching center including a plurality of incoming channels, a plurality of outgoing channels, a plurality of functional modules connected therebetween for transferring all data received by said incoming channels directly to the proper outgoing channels without inspection of the information contained in said received data, at least one of said plurality of functional modules being a computing module and including means for selectively activating the one of said incoming channels having the highest precedence of a predetermined priority, a plurality of subscriber sets, each having an enciphering means, a deciphering means, a digital to voice conversion means and a voice to digital conversion means adapted to receive audio signals and couple its corresponding digital output signals to said enciphering means for entry via one of said incoming channels to said switching center, said digital to voice conversion means similarly adapted to provide audio output signals upon receipt of corresponding digital signals from said deciphering means for exit via one of said outgoing channels from said switching center.

2. The system as set forth in claim 1 wherein each of said subscriber sets includes means for interrupting said received audio input signals and inserting a data word into the incoming stream of audio signals at an interrupting period and rate such as to be substantially harmless to the voice quality of the audio signals.

3. The system as set forth in claim 2 wherein further means are included for inserting into said data word a synchronizing marker code to identify said information as a data word.

4. The system as set forth in claim 3 including further means in each of said subscriber sets for inserting a priority cut-in binary signal into said data word.

5. The system as set forth in claim 4 wherein each of said subscriber sets also includes means for inserting a plurality of talk request signals into said data word.

6. The system as set forth in claim 5 wherein each of said subscriber sets further includes means for inserting into said data word a plurality of conferee-present signals.

* * * * *

UNITED STATES PATENT OFFICE
CERTIFICATE OF CORRECTION

Patent No.___3,674,936___   Dated___July 4, 1972___

Inventor(s)___Fred G. Wolff___

It is certified that error appears in the above-identified patent and that said Letters Patent are hereby corrected as shown below:

The inventor's name is spelled "Fred G. Wolfe" in the heading of the patent. It should be corrected to read -- Fred G. Wolff --.

Signed and sealed this 20th day of February 1973.

(SEAL)
Attest:

EDWARD M. FLETCHER, JR.
Attesting Officer

ROBERT GOTTSCHALK
Commissioner of Patents