A TIME-VARIANT APPROACH FOR ENCRYPTED DIGITAL COMMUNICATIONS

Wai-Hung Ng
The Aerospace Corporation
Los Angeles, California

ABSTRACT

Two new approaches, a time-variant key and a random transmission rate, are introduced to strengthen the security of encrypted digital communications in which a “black-box” type of crypto-device is employed. These approaches not only further upgrade present crypto-methodology, but may also secure the system against the possibility of the cryptographic key’s falling into the hands of an unauthorized listener after initial communication has begun. Therefore, communication privacy could be maintained even under the most scrutinizing post-recorded ciphertext attack.

INTRODUCTION

Communication and storage of information are vital for the advancement of human society and technology. However, it is sometimes desirable to keep certain information confidential; thus, cryptography was devised to keep intruders from comprehending secret messages.

A crypto-system consists of three basic elements: the plaintext (the original message); the key (the specific formula used to encipher the original message); and the cryptogram (the key-enciphered plaintext) [1]. The ideal cryptographic system is unbreakable in common practice, and its key is easy to change and utilize. At the present time, the most popular methods of cryptanalysis (attempts to decipher a cryptogram without knowing the key) are frequency analysis on enciphered symbols and exhaustive trial-and-error computer searching.

Many crypto-devices used in secured digital communication systems contain certain hidden capabilities that, in general, cannot be investigated or modified by users. For this reason, we shall consider any pre-selected crypto-device to be a “black-box” that cannot vary or be altered internally and must be accepted as a

whole. Therefore, further system improvement can be attained only by use of external paths.

Two new approaches, a time-variant key to prohibit exhaustive searching cryptanalysis and a random transmission rate based on a pseudo-random noise (PN) code to prevent an accurate recording of the encrypted signal, are introduced for systems with automatic retransmission capability. These techniques not only strengthen the conventional crypto-system, but also provide the security against an unauthorized listener who has a duplicate of the crypto-device, receiver, time and frequency schedule, and even the crypto-key after initial communication has begun.

As computers become more and more popular, information is more commonly transformed into binary form. For simplicity's sake, this study will discuss only secured binary communications, although it is extendable without restriction to the non-binary situation.

BASIC ENCRYPTED COMMUNICATION SYSTEM CONFIGURATION

The communication system configuration to be investigated in this study consists of a transmitter and a receiver, as shown in Fig. 1. The transmitter is composed of an information source, an encryptor, an error detection/correction encoder, a modulator, and an antenna. Transmission of information proceeds as follows. First, the original information is transcribed into binary form and encrypted into a cryptogram. There is no specific requirement on selecting the crypto-device. For easy reference, we shall assume that a data encryption standard (DES) [2] type of crypto-device is adopted in the system. However, any other crypto-device could be used here without affecting our basic presentation and results. The DES encryptor sequentially maps each block of 64 information bits into a block of 64 enciphered symbols. This process is based on a pre-selected 64-bit encryption key in which 8 bits are used for error detection purpose. Further redundant bits are added to the encrypted sequence through error correction encoding. The coded sequence then is permuted, or scrambled, through a functional extension of the adopted cryptographic key. Finally, the signal is modulated and transmitted through the antenna.

Before demodulating the incoming signal, the receiver must first synchronize the system. Once the received digital signal is accurately acquired, it must be unscrambled through a depermutation process. Then, errors are corrected and detected by channel decoders, and the decryption key is used to derive the original information. One should note that the decryption key may or may not be identical to the encryption key, although the two are identical in DES.

The purpose of our study is to enhance the ability to encrypt digital communications while retaining the preselected crypto-device, cryptographic key, and key entrance technique intact. To fulfill these requirements, a time-varying cryptographic key and a random transmission rate, both controlled by a simple key entrance controlling device external to the crypto-device, are proposed. These two new techniques are simple and easy to implement. They require only a small increase of the system's overall complexity, but the end results can greatly enhance communication security and privacy.

A TIME-VARIANT CRYPTO-SYSTEM

The security of a crypto-system relies entirely on its cryptographic key, and users must prevent the possibility of this key failing into the hands of an unauthorized listener. In other words, we shall assume that only the authorized transmitter and receiver have the crypto-key, and cryptanalysis must rely on trial-and-error computer searching.

In this section, concepts and application procedures of the two new cryptographic techniques are introduced. To simplify the exposition, error detection/correction coding, permutation, modulation, etc., will not be discussed in this study.

The Time-Variant Key

Consider a well-defined encrypted digital communication system containing a "black-box" type crypto-device and a pre-selected cryptographic key, K_{cry}. For a DES-type crypto-system, binary information to be encrypted will be divided into blocks, each consisting of M bits, and the encryption/decryption process will proceed on a block-by-block basis.

The following seven steps explain how to generate and use a time-variant key, K_{tv}. A simple example is given later to illustrate this procedure.

1). We assume that both encryptor and decryptor have a key-entrance controlling device with a small memory to store a set of N pre-determined random keys, where N is determined by available memory size. If each random key has the same length as the cryptographic key, K_{cry}, which is N_{cry} bits long, then each memory will have a size of N x N_{cry} binary bits. For DES, M is also equal to K_{cry}.

2). These N random keys are stored in order in the memory device as K_0, K_1, K_2, ..., K_i, ..., K_{N-1}, and K_i, denotes the decimal value of K_i.

3). The chosen cryptographic key, K_{cry}, is used to start the encryption process.

4). Before generating K_{tv}, we shall first generate a reference key, $K_{ref} = K_{cry} \oplus K_a \oplus K_b$, &, where "$\oplus$" is the modulo-2 addition. Both K_a and K_b are random keys in the memory, with K_a as a function of K_{cry}, and K_b as a function of K_a, where $a = K_{cry}$ (mod N) and $b = k_a$ (mod N).

5). To insure security against the plaintext's becoming all-zero or all-one binary digits, as often occurs in the beginning or ending of each meaningful message signal, the time-variant key K_{tv} is derived by cyclically shifting N_{cyc} positions of the reference key K_{ref} to the left, where N_{cyc} is relatively prime to K_{cry}.

6). This K_{tv} is used to encrypt a block of M binary information bits through the "black-box" crypto-device. After that, a new random key $K_{nt} = K_{tv} \oplus K_c$ is generated, where K_c is a random key in the memory and c = a + b (mod N). Then K_{nt} is shifted into the memory to replace K_0. At the same time, K_0 replaces K_1, K_1, replaces K_2, K_{i-1} replaces K_i, and so forth until K_{N-2} takes on the position of K_{N-1}, and the former K_{N-1} is discarded.

7). In parallel to step 6), the encrypted block of M bits long plaintext, M_m is used to replace K_{cry} and to generate a new K_{tv}. Steps 4, 5, 6, and 7 are then repeated, and the same procedure continuously generates new time-variant keys and encrypts new incoming blocks of plaintext.

Values for N and N_{cry} can be chosen in the neighborhood of 1000 and 64, respectively (i.e., the memory has a size of 64 K-bits), as those adopted in popular personal computers and in DES. Here, we use an oversimplified crypto-system to demonstrate the above procedures.

1). Consider that N = 5 and $K_{cry} = 4$.

2). Select $K_0 = 1001$, $K_1 = 1011$, $K_2 = 0010$, $K_3 = 0111$, and $K_4 = 0101$.

3). Choose $K_{cry} = 1101$. Therefore, a = K_{cry}(mod N) = (1 + 0 + 4 + 8) (mod 5) = 13 (mod 5) = 3, and $K_a = K_3 = 0111$; b = K_a(mod N) = (1 + 2 + 4 + 0) (mod 5) = 7 (mod 5) = 2, and $K_b = K_2 = 0010$.

4). Generate $K_{ref} = K_{cry} \oplus K_a \oplus K_b = K_{cry} \oplus K_3 \oplus K_2 = 1101 \oplus 0111 \oplus 0010 = 1000$.

5). A relative prime to $N_{cry} = 4$ is chosen with the value of $N_{cyc} = 3$. Therefore, we would have $K_{tv} = 0100$.

6). Now K_{tv} = 0100 is utilized to encrypt the new block of incoming plaintext, M_m. This block of M_m is further used to replace the K_{cry} and to generate a new K_{tv}, and so on, as discussed above.

7). At the same time, the generated $K_{nr} = K_{tv} \oplus K_c$ = 0100 $\oplus$ 1001 = 1101 is shifted into the memory to replace K_0, where c = a + b (mod N) = 3 + 2 (mod 5) = 0; we then have $K_0 = K_{nr}$ = 1101, K_1 = 1001, K_2 = 1011, K_3 = 0010, K_4 = 0111. We discard the previous K_4, = 0101 by shifting it out of the memory.

There are three important conceptual issues in this approach. First, the memory device containing N random keys, K_i, is external to the crypto-system. It is independent of the selection and entrance of the preselected crypto-key, K_{cry}, and thus is completely excluded from the key space. Second, it is understood that a particular time-variant key, K_{tv}, can be found from 2^M encryptions in an exhaustive search providing that the corresponding M-bit pair of cipheretext and plaintext is given. However, the knowledge of this K_{tv} alone cannot derive its corresponding K_{cry}, K_a, and K_b, because K_{ref}, the cycling shift of K_{tv}, is only the modulo-2 sum of the three keys. Even if the complete set of random keys, K_i, is given, solutions for K_{cry}, K_a and K_b are not unique and the number of possible solutions is a function of the value of N. Third, assume that N consecutive time-variant keys, K_{tv} and their corresponding keys, K_{cry}, K_a, K_b, can be found by some unspecified techniques. In order to break the code secured by our approach, cryptanalysis still needs to find each of the corresponding K_{nr} which is a function of K_{tv}, K_{cry}, K_a, K_b, as well as to the set of time-variant random keys, K_i.

The concept of time-variant key is not completely new. The Enigma machine [1] used by the German military forces in the Second world war, for example, used a simple time-variant key approach while our approach advanced into techniques of continuously updating its key as a function of encrypted plaintext information. As the real operational key is now changed from a constant key, such as the pre-selected K_{cry}, to a time-variant key, K_{tv}, this approach becomes a useful tool in preventing both the chosen plaintext attack and the corresponding plaintext and ciphertext attack.

Binary Pseudo-Random Transmission Rate

Post-recorded ciphertext attack is the most powerful cryptanalysis method recognized today. In such an attack, the unauthorized listener merely records the cryptograph and then later uses an exhaustive search to break the code. Although many advanced spread spectrum communication techniques, such as direct sequence modulation, frequency hopping, etc., [3] can be utilized to prevent this

attack, a new approach to the same goal with a much simpler implementation is introduced below.

At the present time, advanced digital communication systems usually employ a very high carrier frequency (often selected in SHF or EHF band), and to record the RF analog signal directly would subject to reduce the S/N ratio significantly and further introduce new transition errors. To record the incoming signal accurately, the recording must be conducted in the baseband, not in the modulated carrier waveform. Since only fixed transmission rates are employed in present communication systems, an unauthorized listener may be able to demodulate the incoming signal into a baseband signal and record it for later cryptanalysis once the bit synchronization has been correctly derived from the received signal.

Let us consider an n-bit-long shift register, where $n \leq N_{cry}$, whose initial binary setting digits are exactly the same as the first n digits in the pre-selected K_{cry}. By using a proper feedback hookup, a PN sequence with a maximum period of $(2^n - 1)$ bits can be easily generated. Then each binary bit in this generated PN sequence can be further used as a reference to produce a new system whose transmission rate is also time-variant.

Assume that the original transmission rate of a system is R-bits/sec such that each bit has a duration time of (1/R) seconds. Based on each digit in the generated PN sequence, a variable transmission rate can be conducted as follows.

Consider that the generation of PN code, S, and the encryption of plaintext, M_m, are processed parallelly. If the newly generated PN code bit is a “0”, the bit duration time is changed from (1/R) to $(1 - \Delta) \times (1/R)$; and if the newly generated bit is a “1”, the bit duration time is changed from (1/R) to $(1 + \Delta) \times (1/R)$, where Δ ranges from 0.05 to 0.1. Therefore, the overall transmission rate remains unchanged. For easy reference, an example to illustrate how the transmission rate varies with the PN sequence digits is given in Fig.2.

Transmission of digital signals customarily starts with a preamble, or a known pattern, prior to sending the binary information sequence. Based on this preamble, the receiver synchronizes its clock and frequency with the receiving signal. To acquire an accurate bit-synchronization, it requires a correct estimate of both the bit transitions and their regularity [4]. However, without the precise knowledge of the initial setting digits (i.e., the pre-selected cryptographic key, K_{cry}) of the PN code, it would not be feasible to recover the bit transitions correctly and to derive the bit synchronization precisely. Thus, the receiver will not be able to record and demodulate the baseband signal accurately. Also, it is obvious that recording a

long sequence with variable transmission rate will definitely cause many bit-slipping events.

Without knowing the pre-selected K_{cry}, the only possibility to record the RF analog signal and use it to determine the variable transmission rate is to assume the bit duration time to be Δ/R seconds. However, there are two main drawbacks in this approach. First, the noise bandwidth will increase $1/\Delta$ times, and thus results in a minimum of 10 dB reduction in the S/N ratio. The practical margin designed for modern communication systems is quite conservative, thus this reduced S/N ratio will unavoidably result in an extremely poor reception. Second, compared with normal random transmission signals, the number of bit transitions is reduced $1/\Delta$ times, and at most one transition can appear in every consecutive $2/\Delta \geq 20$ bits of duration time. In this case, it will be very difficult for the receiver to obtain its correct bit synchronization. Therefore, accurate recording should only be conducted with the demodulated baseband signal, and not with the RIF analog signal.

When a system adopts the binary PN variable transmission rate, the probability of bit-slipping for demodulating the incoming signal with constant bit rate could be quite high. For example, a bit pattern with 6 all-zeros, or 6 all-ones, is expected to occur in any PN sequence with length of 2^6 - I = 63 bits. Now, if each code bit varies its transmission rate with Δ = 10%, a 6 consecutive equal bit pattern would vary the total bit-duration time from constant transmission rate of requiring 6 x (1/R) seconds to either 6 x (1 - Δ) = 5.4 x (1/R) seconds which could be acquired as 5 bits, or to 6 x (1 + Δ) = 6.6 x (1/R) seconds which could be acquired as 7 bits. In other words, if bit synchronization is derived from majority decision rule, then a bit-slipping event is expected to occur in every block of 63 evenly recorded information bits. Once a bit slipping or a receiving error occurs in a cryptographic system, the damage is done and catastrophic effects grow out of control. Hence, combination of the proposed two approaches is a powerful tool in combatting the cryptanalysis.

DISCUSSIONS AND CONCLUSIONS

The proposed new methods of a time-variant key with a random transmission rate could be important advancements for future crypto-systems. Basically, only three additional components are needed to implement these two techniques. They are (i) a key entrance controlling circuitry, (ii) a small N x K_{cry} bit memory, and (iii) an n-bit long shift-register. Therefore, the required hardware is indeed relatively simple.

We recommend that these two new approaches be adopted in two-way communication systems with automatic retransmission capability. In this system, continuity of the transmission depends on the receiver's acknowledgement of correct reception. If the receiver's feedback is incorrect, the sender should stop sending the remaining message and retransmit the previous message until acknowledgement of correct reception is received. Detailed investigations and discussions on automatic request retransmission are available in the literature [5].

REFERENCES

[1]. Konheim, A. G., Cryptography: A Primer , John Wiley & Sons, Inc., 1981.

[2]. National Bureau of Standards, "Data Encryption Standard," Washington, D. C.: NTIS, January 1977.

[3]. R. E. Ziemer and R. L. Peterson, Digital Communications and Spread Spectrum Systems , Macmillan Publishing Co., New York, 1985.

[4]. W. H. Ng, "Analytical Study on Bit-Synchronization Problems in A Coded Communication System," ITC Proceedings, pp. 551-554, 1984.

[5]. S. Lin, D. J. Costello, Jr., and M. J. Miller, "Automatic-Repeat-Request Error-Control Schemes," IEEE Communications Magazine, pp. 5-17, 1984.

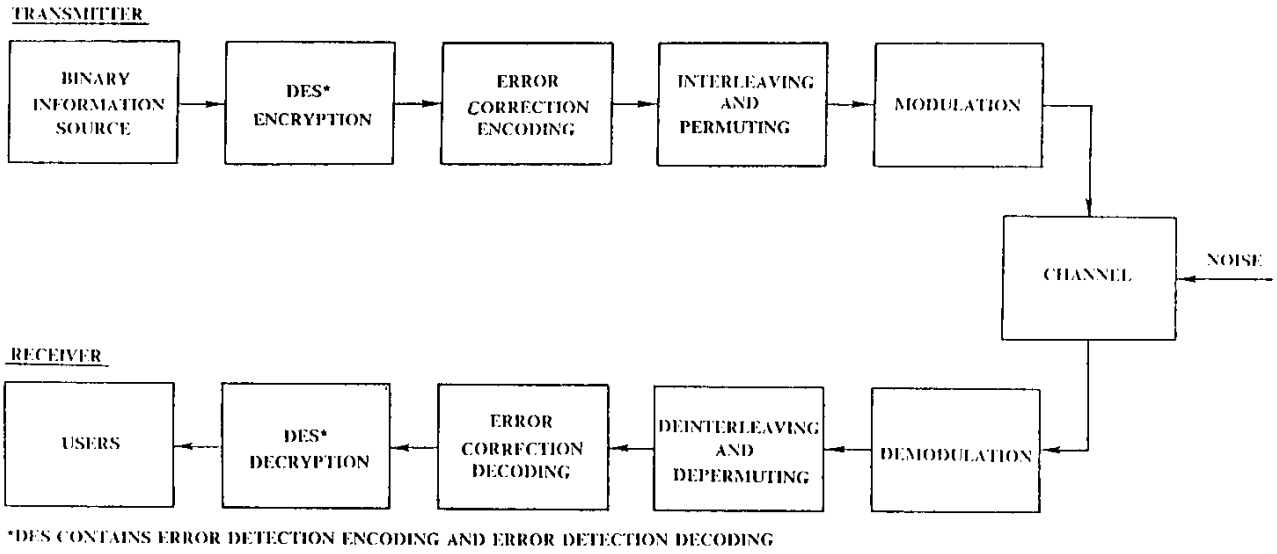
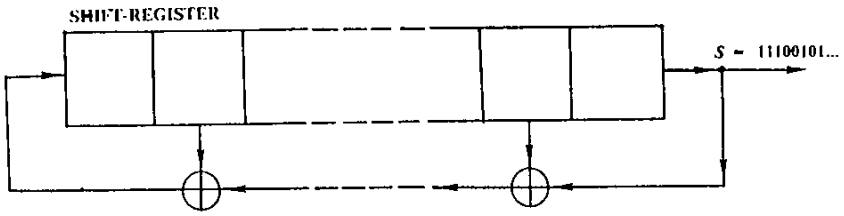
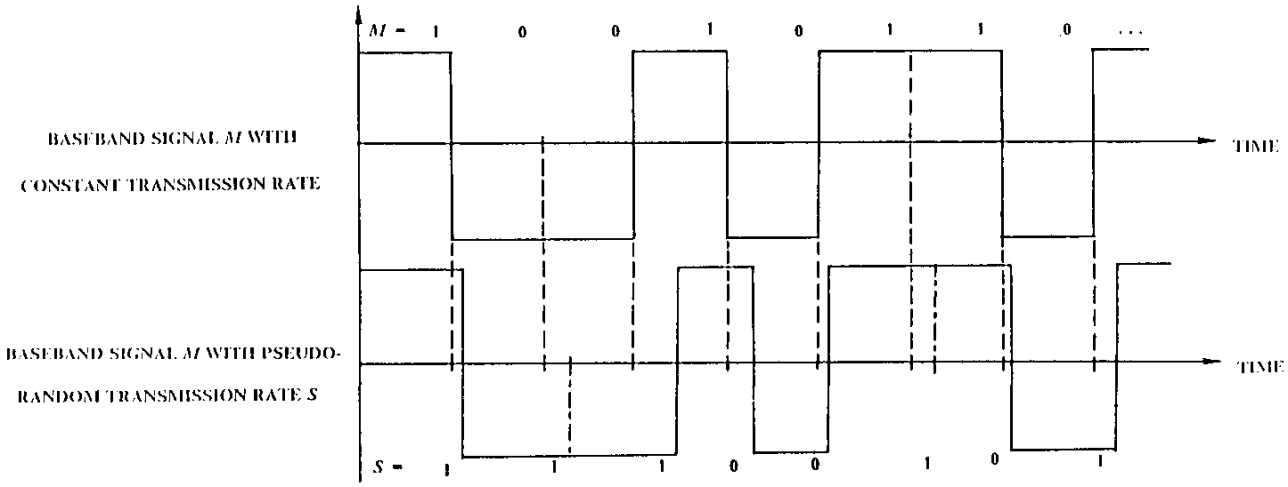


FIGURE 1 BASIC ENCRYPTED DIGITAL COMMUNICATION CONFIGURATION



a. Generation of Binary Pseudo-Random Sequence S



b. Baseband Signal with Given Transmission Rate

FIGURE 2 GENERATION OF BASEBAND SIGNAL WITH VARIABLE TRANSMISSION RATE