ENCRYPTION AND KEY MANAGEMENT FOR THE ECS SATELLITE SERVICE

Serpell, S.C., and Brookson, C.B.

British Telecom Research Laboratories, Martlesham Heath, Ipswich, Suffolk. IP5 7RE.

ABSTRACT

This contribution describes the encryption and key management techniques realised with prototype hardware by British Telecom Research for use on the SatStream service offered on the European Communication Satellite. The security objectives, channel unit functions and operation, encryption methods and key management systems are described.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 426-436, 1985.

INTRODUCTION

British Telecom International's European SatStream service (1) will offer business telecommunications by satellite. This service will include digital single-channel-per-carrier and continuous mode frequency division multiple access links via the European Communication Satellite (ECS). The broadcast capability of SatStream allows customers' transmissions to anywhere in Europe with relatively small and cheap earth stations. This is a significant advantage over the terrestrial network, but at the same time it makes the links more vulnerable to eavesdropping.

The unauthorised reception of SatStream traffic would require considerable expertise and financial investment; nevertheless it was decided to develop an optional encryption facility to provide for the total security of sensitive customer data when this is required. This facility renders the data on the SatStream link entirely unintelligible to all except the intended recipient stations. Similar encryption facilities have been defined for the United States Satellite Business Systems (2) and French Telecom 1 (3) business satellites.

SECURITY OBJECTIVES

The SatStream encryption scheme is designed to meet the following security objectives:

- -To render customer data transmissions unintelligible to unauthorised receivers,
- -To prevent inadvertent transmission of unencrypted data even under equipment failure conditions,
- -To prevent theft, unauthorised use, or unauthorised modification of cryptographic equipment while installed,
- -To prevent unauthorised disclosure or modification of sensitive data (plaintext, unencrypted key-variables....) while in cryptographic equipment,
- -To support secure key-variable generation and key-variable management.

These principles were kept constantly in view during the design of the earth station baseband channel units which incorporate the encryption facility.

CHANNEL UNIT BASEBAND FUNCTIONS

The British Telecom baseband channel unit for the SatStream service consists of transmit and receive half units. Each half unit may be used independently of the other, and this is of importance since one of the SatStream service options requires the ability for one transmitter to broadcast to a number of receive-only stations.

The transmit half unit performs the following functions:

- -Synchronisation to the incoming user data, which may be in CCITT G703 format (64 kilobits per second codirectional) , X21 format (nx64 kilobits per second, where n = 2 to 30), or G732 format (2.048 Megabits per second),
- -Conversion of the incoming data to a G732-like framed structure if it is not already in that format,
- - Calculation of the encryption parameters and insertion into the G732-like format at multiframe level,

-Encryption of the user data,
-Transmission of the encrypted data in the G732-like multiframe format.

The receive half of the unit performs a complementary set of functions to those of the transmit unit, namely:
-Synchronisation to the incoming data with the G732-like multiframe format,
-Recovery of the encryption parameters from the multiframe structure,
-Decryption of the data,
-Output of the recovered data in its original G703, X21 or G732 format.

A block diagram of these functions is set out in figure 1. Some further baseband processing is also performed on the data before it is passed to the earth station modulator or received from the demodulator, in particular half- rate error protection using the Viterbi Forward Error Correction algorithm is applied to all data. Data is also scrambled to remove long strings of binary '1's or '0's, or short cyclic periodic structures embedded in data, since data with these characteristics would cause problems over the satellite link.

FRAME AND MULTIFRAME STRUCTURE

All data flowing over SatStream links is structured into a format similar in conception to the CCITT G732 specification as used in the 30 channel Pulse Code Modulation (PCM) systems in the terrestrial network, but with certain important modifications. This structure is used to advantage to the ensure reliable operation of the encryption system.

The structure is shown in figure 2. Each data frame comprises 64 time slots (or bytes) of 8 bits each, thus each frame is effectively a 'double' G732 frame (one 'odd' plus one 'even' frame in G732 terminology). All the time slots within the frame contain customer data apart from four time slots reserved for special purposes. These are time slot (TS) 0, which contains the frame unique work, TS16 with TS48, which may be used for signalling information, and TS32, which contains message fields.

The 512-bit frame thus contains (64-4)x8=480 bits of customer data. Customer data presented in G703 or X21 format is therefore subject to an expansion of 32/30 over the satellite path, while data already in G732 format remains unexpanded. The frame unique word contains a fixed 7 bit code, the presence of which denotes the first time slot of a new frame.

A multiframe is defined as 64 frames, and a fixed multiframe unique word is carried in time slot TS32 during the course of the multiframe. Other TS32 bits are used to convey Initialisation Vectors (IVs) for encryption synchronisation, the identification of the encryption key-variable in use, and the identification of the transmitting station (16 bits) and station channel unit (8 bits).

ENCRYPTION FACILITY

Design

The encryption facility on the channel unit is designed for very high security against attack by an adversary. This security derives from the digital encipherment of the customer data using a complex algorithm in stream cipher mode under the control of long, random key-variables.

Encryption method

The method of encryption is shown in figure 3. The customer data (or "plaintext") is "Exclusive ORed" with a randomising pattern (or "key-stream") from the cryptographic engine to produce an unintelligible output ("ciphertext"). Synchronised 'Exclusive ORing' of an identical key-stream at the receive end of the link will then regenerate the plaintext. This process is termed "stream ciphering" and is well-suited to SatStream because the resulting encryption is transparent to customer data and it has no error extension property. Each error on the enciphered satellite path causes only one error in the deciphered plaintext. This is essential in a satellite application when high error rates are the rule in fading conditions. The stream cipher mode is not self-synchronising and an overhead is incurred as a result.

The equipment on the transmit side thus structures the data and forms the ciphertext using keystream output from the cryptographic engine, while the receive unit disassembles the frame and applies the converse operation to recover the plaintext. The keystream pattern is controlled by the cryptographic algorithm, the contents of the cryptographic engine input register, and by the secret key-variable. These are discussed in turn below.

Algorithm

The security of the encryption facility is made to depend only on the key-variable in use by selecting a sufficiently strong cryptographic algorithm. Following normal cryptographic philosophy the SatStream facility has moreover been designed so that it is impracticable for an adversary to deduce a key-variable even given full knowledge of all the hardware and quantities of matched plaintext and ciphertext ("Known plaintext attack"). In particular, the number of possible key-variables is so large that it is computationally infeasible for an adversary to discover the key-variable in use by exhaustive search.

The United States' Data Encryption Standard (DES) was considered for this application but would have caused difficulties in supply and uncertainty regarding intellectual property. An alternative, unencumbered, algorithm was made available by British Telecom Cryptographic Products, which was internationally adopted for exclusive use on the SatStream service. This algorithm has been called TACA (Telecommunications Administrations Cryptographic Algorithm) and uses a 96 bit key-variable.

Encryption synchronisation

Correct decryption of an encrypted transmission in the stream cipher mode requires the synchronised addition of identical keystreams at both ends of a link. In particular this implies the maintenance of identical entries in the cryptographic engine input registers at transmit and receive ends of a link. In traditional point-to-point duplex links, this may be accomplished by bidirectional set-up protocols. However, SatStream services must also support unidirectional and broadcast (point to multipoint) links, and new receiving stations must be able to join a network without disturbing other network stations. This problem is overcome by controlling the encryption synchronisation entirely from the transmit end of the link, through the generation and transmission of an Initialisation Vector (IV) on each path every multiframe. The IV is used to force into a new synchronisation the state of every receiving cryptographic engine at the start of each multiframe. Thus any receiving station joining into an existing network for the first time, or rejoining the network after a service break, is assured of rapid synchronisation with the transmitting station. This technique may also be used to allow multi-destinational links.

If for any reason the transmit and receive ends of a link use different IVs, a different keystream is then applied to the customer data and a 50% error rate results. It is consequently essential that IVs are strongly error protected in transmission since each incorrect IV reception will cause the loss of one complete multiframe of customer data. Further complications arise from the presence of the Viterbi convolutional coding units on the satellite side of the encryption units. The Viterbi units generally improve the error rate greatly by correcting most of the Gaussian-type errors occuring on the space path, but occasionally produce lengthy error bursts. The IVs are therefore protected by:

- -The Viterbi units,
- -The addition of a (12,8) shortened Hamming block code capable of correcting single errors within any sequence of 8 IV data bits,
- -The spacing of the Hamming code protected IV bits so that a typical Viterbi-type error burst cannot affect more than one bit of any 12 bit block.

These combined measures render the probability of erroneous IV reception negligible.

Key-variable synchronisation

The same keystream is only produced so long as the same key-variable as well as the same IV is in use at both the transmit and receive station. The key-variables are changed on a regular basis to prevent too much customer data being committed to any one key-variable. Synchronised changeover of key-variables is therefore required and this is achieved by associating an identification number with each key-variable. This number is continuously signalled by the transmit station. The key-variable

changeover is automatic and initiated by the transmission of a new key-variable identifier. The encryption facility retains a store of key-variables in semiconductor memory. This allows long periods of secure and continuous operation before a new batch of randomly generated key-variables need be loaded into the encryption unit. The system is further designed so that during this period of dynamic key-variable change there are no service interruptions or corruptions of the customer's data.

The key-variable identifiers not only benefit from all the protection afforded to the IVs, but in addition the the receiver unit will only change to a new key-variable on the receipt of a two identical key-variable identifiers which differ from that of the key-variable presently loaded into the encryption engine. As each key-variable is exhausted it is overwritten and no trace remains within the encryption unit, preventing any possible retrospective reading of the key-variables.

KEY MANAGEMENT

A key-variable management scheme has been designed and built to allow for the secure generation of encryption key-variables from a truly random source and their secure handling and distribution, and to ensure that the correct key-variables are loaded into the correct equipment in a timely manner.

International

The European offering of SatStream using the European Communication Satellite will allow the encryption of international as well as national satellite links. International key-variable distribution will be achieved in a secure manner, with key-variables being protected in transit by a one-time pad. International key-variable distribution may also use the more automated system described below, which was designed to simplify UK national key management.

UK National

The key-variables are distributed to the earth station encryption units by key guns or key transfer devices. The key guns are small hand-held devices capable of holding up to 16 batches of key-variables with a self contained liquid crystal display displaying the station and channel identification for each batch. The key guns themselves are previously filled with key-variables either at a secure key management centre or at a remote location connected to a key management centre by secure and encrypted links. Key-variables are generated at key management centres using a true random process and are checked against known undesirable key-variables to eliminate any unfortunate values. Figure 4 shows the key management scheme. A small computer system is used as the principal key management unit.

The key-variables are loaded into the encryption units from the key guns via a short physical wire link when a manually initiated request is received from the encryption unit, subject to certain physical controls to prevent unauthorised operation.

SECURITY FEATURES

The security of the earth station encryption unit and the key management system are important considerations in a system such as that developed for SatStream. The encryption unit is incorporated into the channel unit from the initial design phase, and it is protected by being encased within a tamper resistant module securely embedded within the surrounding equipment.

Key-variable security

Key-variables may not be read out of the tamper resistant module. This module will, on the detection of any tampering or attempted removal from the surrounding units, completely erase all key-variables contained within itself, while simultaneously raising system alarms. Similar considerations have also been applied to the key gun, and in this case a facility is also provided for complete erasure of all sensitive data by manual operator action.

Bypass

The encryption unit has been so designed that it contains no physical or logical internal bypass paths, since these could potentially allow transmission of unencrypted data. Under certain failure conditions transmission equipments transmit AIS or 'All-Ones' in place of customer data, and this failure signal must appear to pass transparently through the entire system including the encryption unit. Since the unit has no internal bypass circuits an AIS generator is incorporated which takes over the encryption unit output if AIS is detected at the input. The exclusion of any bypass capablity ensures that under no conditions can any unencrypted customer data be transmitted.

Transmission in depth

The security of the data is compromised if the same cryptographic engine input register state occurs more than once within the lifetime of any given key-variable ('Transmission in depth'). Special methods are used in the generation of IVs to overcome this problem.

TESTS

The design and operation of the channel unit equipment and associated key management principles have been thoroughly tested in both laboratory tests and using satellite links over the Orbital Test Satellite (OTS). The encryption methods employed have proved to be highly robust and able to accomodate the severe carrier-to-noise characteristics encountered on space paths, with the synchronisation and error correction facilities performing exactly as those which were predicted. The encryption facility has been proven not to affect the overall channel error rate.

CONCLUSIONS

The optional encryption facility developed for the European SatStream service offers a very high level of security on the

satellite path, backed up by good equipment physical security, sound key-variable generation, distribution and management. It uses redundancies within the SatStream G732-like data structure and so does not require expansion of the existing frame structure. It is completely transparent to customer data and has no effect on channel performance. It permits unidirectional and multidirectional (point-to-point and -multipoint) encrypted links without the need for reconfiguration if the number of participating stations changes, and represents a considerable service enhancement for users concerned about the sensitivity of their data.

ACKNOWLEDGEMENTS

Acknowledgement is made to the Director of Research, British Telecom, for permission to publish this paper.

This paper was presented at the IEE International Conference on 'Secure Communication Systems', London, 22nd-23rd February 1984. Copyright of this paper is held by the IEE and acknowledgement is made to the IEE for permission to publish this paper.

REFERENCES

1. McGovern,D., and Kernot, R.J.,"A Second-Generation SCPC System for Business Satellite Communication", September 1983, 6th International Conference on Digital Satellite Communications, Phoenix, Arizona, USA, III-12 to III-17.

2. Stein, F.L., "An Integrated Multiple Transponder TDMA Bulk Encryption Satellite Communications System", September 1983, 6th International Conference on Digital Satellite Communications, IX-16 to IX-20.

3. Bic,J.C., Bousquet,J.C., and Oberle,M., "Privacy over Satellite Links", 23-26 March 1981, Proc. 5th International Conference on Digital Satellite Communications, Genoa, Italy, 243-249.

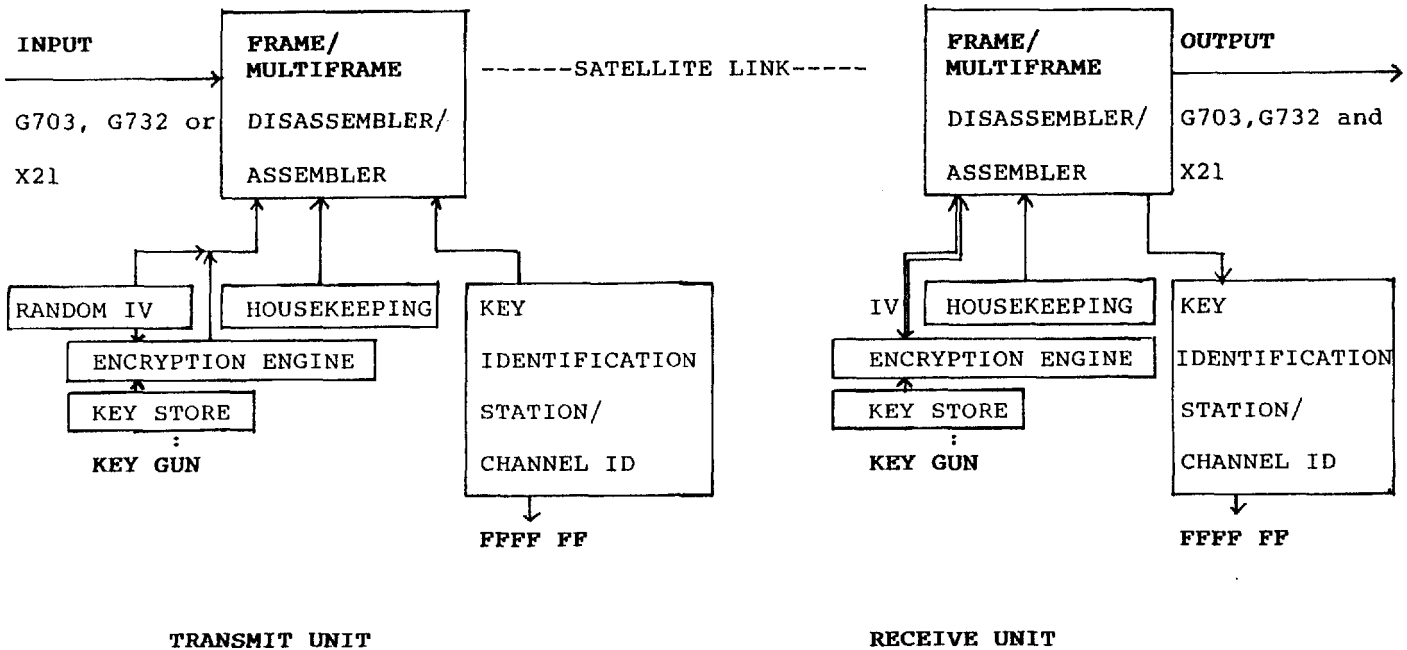
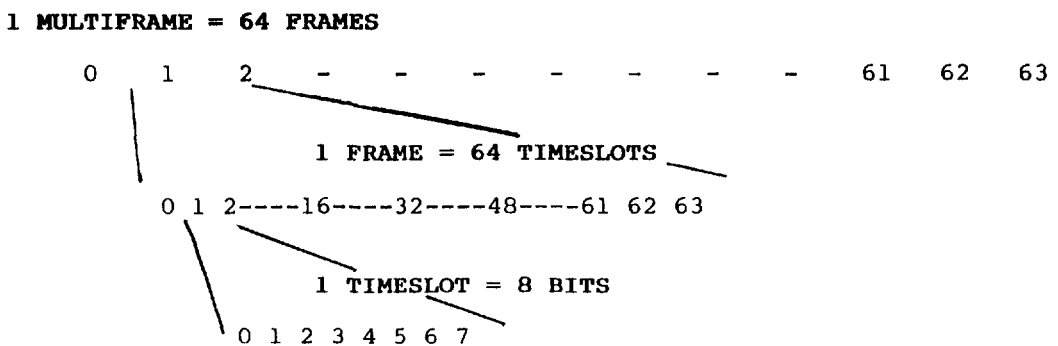


Figure 1. Channel unit schematic diagram



TS0 : FRAME UNIQUE WORD - 0 0 1 1 0 1 1
TS16: SIGNALLING FIELD
TS32: MESSAGE FIELD R 1 R R R R R R *
TS48: SIGNALLING FIELD

* R- Reserved bits for the multiframe unique word, channel and station identifiers and encryption parameters.

Figure 2 Data format

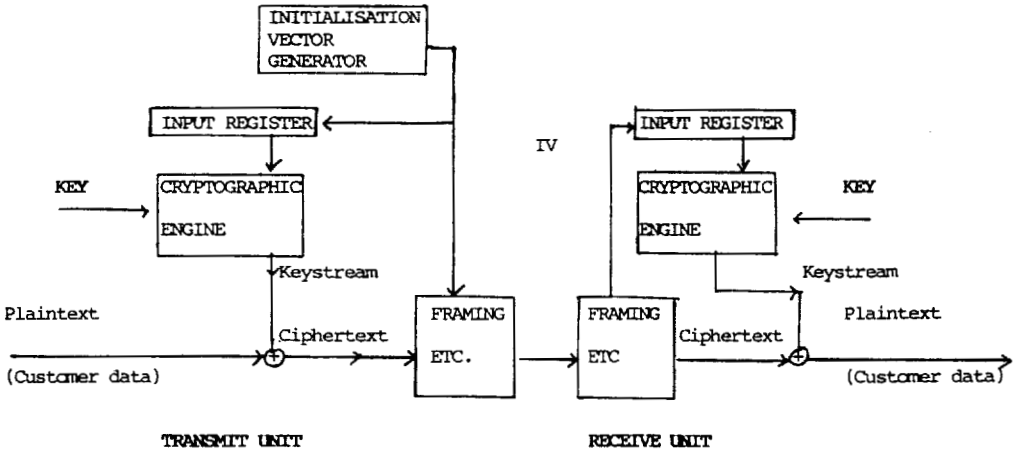


Figure 3 Encryption functions of the channel unit

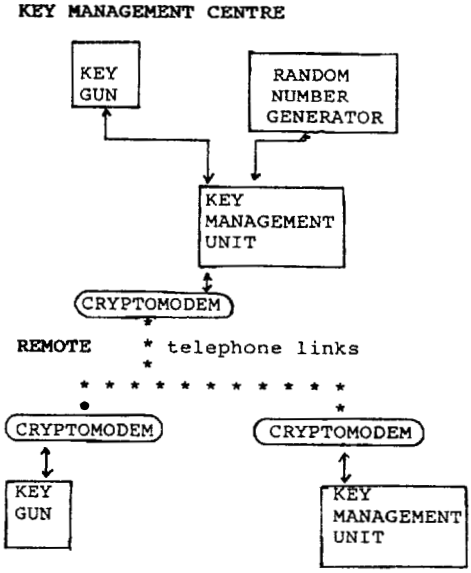


Figure 4 Key management scheme