Crypto-Coding as RSA-Turbo for Land Mobile Satellite Channel

Rajashri Khanai
Department of Electrical and Electronics Engineering, Gogte Institute of Technology, Belgaum, Karnataka, India
Email: rajashri.khanai@gmail.com

G. H. Kulkarni
Department of Electrical and Electronics Engineering, Jain College of Engineering, Belgaum, Karnataka, India
Email: ghkulkarni1@rediffmail.com

Dattaprasad A. Torse
Visvesvaraya Technological University, Belgaum, Karnataka, India
Email: torseda@gmail.com

***Abstract*—Fading in wireless media is a major difficulty in reliable communications, hence secured data transmission over an unreliable channel needs an additional step of error-correction coding. In this paper we have proposed the Crypto-Coding technique that combines encryption and error-correction as a single primitive. Here turbo code is embedded in public key cryptographic algorithm such as Rivest-Shamir-Adelman (RSA) to achieve security and reliability into a single step. The combined system's performance is evaluated on Land Mobile Satellite (LMS) Channel. The results are compared with the system using ideal encryption and decryption.**

***Index Terms*—crypto-coding, interleavers, land mobile satellite (LMS) channel, turbo coding, rivest-shamir-adelman (RAS)**

I. Introduction

The question of combining cryptography and error correction was dealt by McEliece for the first time [1]. Since then, unfortunately, very few researchers have tried to deal with this problem. Some authors argue that a crypto-coding has not fascinated more attention since the fact that error correction introduces redundant data (i.e. data expansion), which is usually not agreeable in cryptography. However, when secured data is transmitted over a noisy channel, then redundancy plays very important role in the correction of corrupted data at the decoder. In that circumstances the combined computational costs of First-Encryption-Then-Coding which usually referred as traditional approach bigger than those required by the crypto-coding procedure.

In addition to decreasing computational costs, we discuss another advantage that one crypto-coding system may pose. Namely, we refer to the recently proposed cryptcoding system [2] which can have arbitrarily chosen redundant information. More precisely, the system is defined in a way that the redundant information used for error-correction is not pre-determined by the nature of the error-correction part of the algorithm but it can be chosen arbitrarily out of the whole set of possible strings. In this paper, we propose a new scheme as crypto-coding. Turbo code is embedded in Rivest Shamir Adelman (RSA) encryption algorithm to reduce computational costs. Secured data is efficiently transmitted over Land Mobile Satellite (LMS) channel with the help of turbo code having different interleavers.

II. Turbo Code: Encoding with Interleaving

A. Channel Coding

Channel code design is always a trade-off between bandwidth and energy efficiency. Codes with lower rate i.e. with larger redundancy can generally correct more errors. If more errors can be corrected, then transmission can happen with low power for long distance, tolerate more interference, and transmit at a higher data rate. These issues make the code energy efficient. Also the complexity in decoding increases exponentially with code length, and hence computational requirements. This is the central problem of channel coding, according to Viterbi stating that encoding is easy but decoding is inflexible [3].

The theoretical upper limit on the data transmission rate called as channel capacity C, for which error-free data transmission is possible is given by Shannon's channel capacity (after Claude Shannon, who introduced the notion in 1948). For additive white Gaussian noise channels, the formula is

$$R < W\log_2\left(1+\frac{S}{N}\right) \text{ bits/sec} \quad (1)$$

In practical situations, there is of course no channel which can be called as an ideal error-free channel. Instead, error-free data transmission is interpreted in a way that the

Manuscript received December 13, 2013; revised May 14, 2014.

doi: 10.12720/ijeee.3.2.121-128

bit error probability can be brought to an arbitrarily small constant by error correction coding. The bit error rate (BER) used in benchmarking is often chosen to be 10^{-5} or 10^{-6}.

Since 1993, the inheritance of turbo codes has released latest technical research areas continuously. It flickers several new ideas to improve its own performance. Furthermore, its concept is integrated with other communication techniques in order to improve by and large system performance. The effect of turbo code has the following examples [4];

- Turbo product codes/Turbo block codes
- Turbo equalization
- Turbo codes for multilevel or turbo trellis coded modulation (TTCM)
- Space-Time turbo codes
- Low-Density parity-check codes (LDPC)

B. Encoder

The general structure of binary turbo encoder by means of two component encoders is shown in Fig. 1.

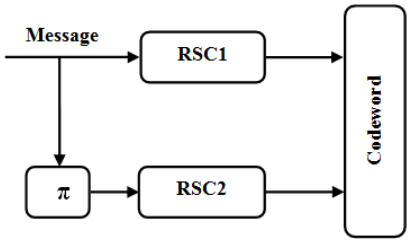

Figure 1. The generic turbo encoder block diagram

The basic building blocks of turbo code are: encoders and an interleaver π with a multiplexing unit to generate the codeword. The component encoders are RSC (Recursive Systematic Convolutional encoder) encoders. In systematic codes, the message will be the part of codeword, which corresponds to a direct connection from the input to one of the outputs. Such an encoder with code rate $\frac{1}{2}$ is depicted in Fig. 2.

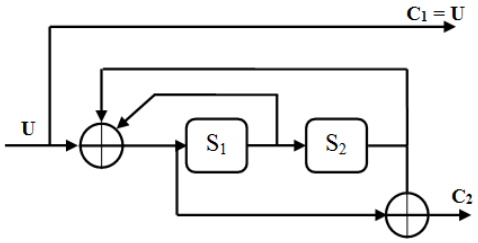

Figure 2. Recursive systematic convolutional encoder, code rate ½

The recursive encoder will be defined by

$$G_{sys}(D) = \left(1, \frac{g_1(D)}{g_0(D)}, \ldots\ldots, \frac{g_{n-1}(D)}{g_0(D)}\right) \quad (2)$$

The generator polynomials of the above figure are $g_0(D) = 1 + D + D^2$ and $g_1(D) = 1 + D^2$.

C. Interleavers

The main role of an interleaver is to scatter the sequences of bits in a data-stream which reduces the effect of burst errors introduced in transmission. An interleaver is usually used in combination with some type of error correcting code like turbo code. The typical sources of burst errors are listed below:

- Wireless communications is severely affected by Channel fading and distortion
- Lightening and switching
- Concatenated coding schemes, usually generates a burst errors where the decoding such as Viterbi fails.

The different types of interleavers used in this paper are relative prime, random and S-random.

- Relative prime interleaver plays around a prime number. For a block size K, a prime interleaver can be constructed by defining a prime number p, as shown

$$\pi(i) \equiv (\pi(i-1) \times p) \bmod K \quad (3)$$

Here the block size K is divided in two parts k_1 and k_2 such that $K = k_1 \times k_2$.

- Random interleaver is the one which is generated by randomly selecting the addresses over a range of block size K. They do not have any standard structure and the main disadvantage is that once generated through some random function that cannot be reproduced again. Hence the only way to use them in actual hardware is to memorize the sequence by Look Up Table (LUT), but they perform very well against any kind of the burst errors.
- The semi-random interleaver named as S-random interleaver [5] is also a type of random interleaver with conditions applies on randomly selected addresses. The generation of address sequence for S-random interleaver is as follows:
- First element of the interleaver randomly select from the range $\{0,1,2,\ldots\ldots K-1\}$, where K is the block size.
- For each next randomly selected element, check that it is $\geq S$ distance apart from previously selected S elements. If it does not satisfy the condition, discard it and repeat the step with next randomly selected element.
- If it satisfies the condition, take it as a member in the interleaver sequence, and proceed until complete sequence has been generated [5].

D. Turbo Decoder

The decoder is made up of two elements decoder1 and decoder2. Decoder1 associated with de-interleaver produces partial output and after spreading errors decoder2 decodes remaining output with second de-interleaver.

The decoder is implemented using decoding algorithm introduced by Bahl, Cocke, Jelinek and Raviv (BCJR).

Because of complexity the BCJR does not have any advantage over Viterbi algorithm. However, as it uses soft-input-soft-output (SISO) decisions it becomes

decisive factor and helps in iterative decoding of turbo codes [6].

The description of the BCJR algorithm is based on log-likelihood ratios (LLR). The LLRs are symbolized as follows. This algorithm determines the probability that a given transmitted bit is ***+1*** or ***-1***, depending on the received sequence $L(b_i/Y)$. The LLR $L(b_i/Y)$ summarizes these two probabilities by calculating a unique number

$$L(b_i/Y) = ln\left(\frac{P(b_i = +1/Y)}{P(b_i = -1/Y)}\right) \quad (4)$$

The Bayes rule is used to express the above equation as

$$L_e(b_i) = ln\left(\frac{\sum_{\{u',u\}?_i} \alpha_{i-1}(u')\gamma_{i\text{-}extr}(u',u)\beta_i(u)}{\sum_{\{u',u\}?_i} \alpha_{i-1}(u')\gamma_{i\text{-}extr}(u',u)\beta_i(u)}\right) \quad (5)$$

$$= C_2 e^{E_b/\sigma^2} \sum_{k=1}^{n} (y_{ik}, x_{ik})$$

here the symbol ***'0'*** is transmitted through the channel as ***-1***, and symbol ***'1'*** is transmitted as ***+1*** *and* the use of polar format is usually convenient for decoders which make use of LLRs [7].

The bit probability of the i^{th} transition is calculated by the expression,

$$P(b_i) = P(b_i = \pm 1) = \frac{e^{L(b_i)/2}}{1 + e^{L(b_i)/2}} e^{b_i L(b_i)/2} = C_1 e^{b_i L(b_i)/2} \quad (6)$$

If transmission is done in polar form then transmitted bits X_{ik} take the normalized values +1 and -1,

$$L_e(b_i) = ln\left(\frac{\sum_{\{u',u\}?_i} \alpha_{i-1}(u')\gamma_{i\text{-}extr}(u',u)\beta_i(u)}{\sum_{\{u',u\}?_i} \alpha_{i-1}(u')\gamma_{i\text{-}extr}(u',u)\beta_i(u)}\right) \quad (7)$$

$$= C_2 e^{E_b/\sigma^2} \sum_{k=1}^{n} (y_{ik}, x_{ik}) \quad (8)$$

The expression for calculating coefficients $\gamma_i(u',u)$ is finally

$$\gamma_i(u',u) = C e^{b_i L(b_i)/2} e^{\frac{E_b}{\sigma^2}\sum_{k=1}^{n}(y_{ik}, x_{ik})} \quad (9)$$

III. RIVEST-SHAMIR-ADELMAN (RSA)

Asymmetric algorithms rely on one key for encryption and other but related key for decryption. Such algorithms have the following important characteristic.

It is computationally infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and the encryption key.

A public-key encryption scheme has six ingredients:

- *Plaintext* is the readable message information or data that is fed to the algorithm as input.
- *Encryption algorithm* performs various transformations on the plaintext.
- *Public and private keys:* This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input [8].
- *Ciphertext* is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertext.
- *Decryption algorithm* takes the ciphertext and the matching key and produces the original plaintext [9].

The public key encryption schemes are as shown in following figures. Fig. 3 gives the encryption with public key and Alice decrypts the message with his private key. In Fig. 4 Bob encrypts with his private key and Alice decrypts that message with public key as mentioned in the following figures.

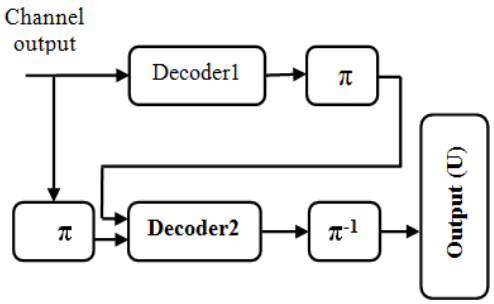

Figure 3. The generic turbo decoder Block Diagram.

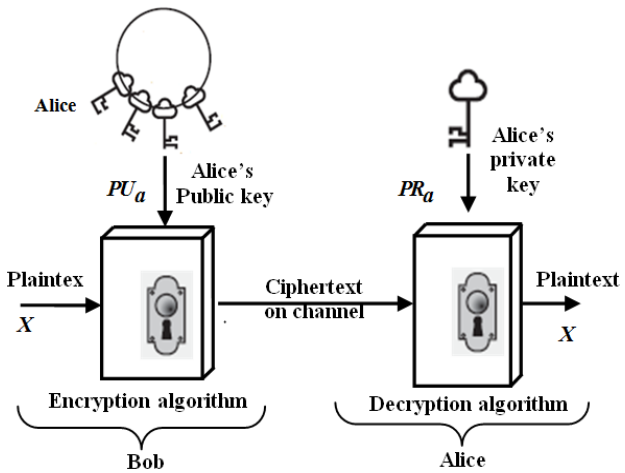

Figure 4. Encryption with public key

In Fig. 4, the encryption and decryption of messages are performed as

$$\text{Encryption: } Y = E[PU_a, X] \quad (10)$$

$$\text{Decryption: } X = D[PR_a, Y] \quad (11)$$

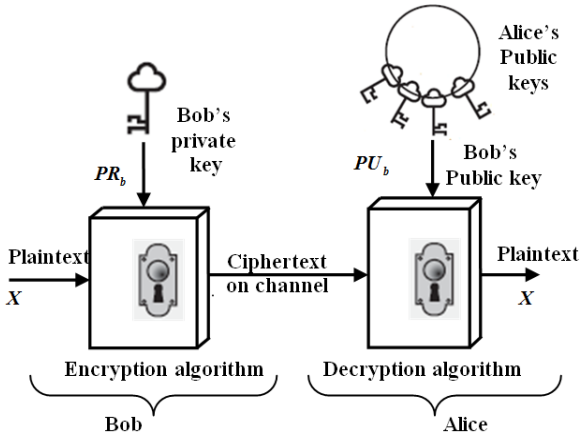

Figure 5. Encryption with private key

In Fig. 5, the encryption and decryption of messages are performed as

$$\text{Encryption: } Y = E\left[PR_b, X\right] \tag{12}$$

$$\text{Decryption: } X = D\left[PU_b, Y\right] \tag{13}$$

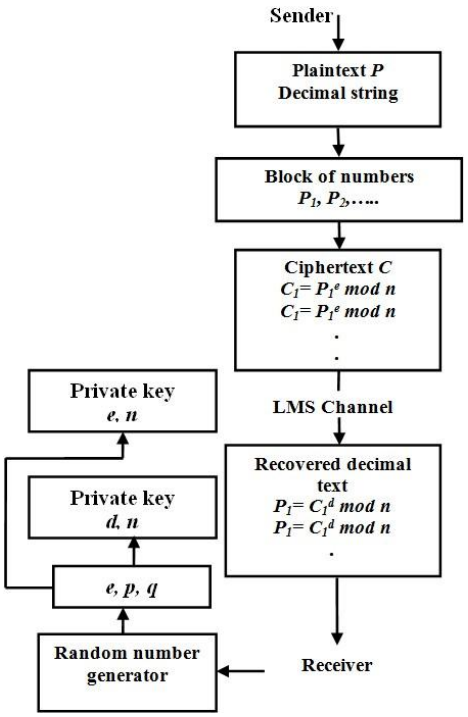

Figure 6. RSA encryption and decryption structure.

The steps involved in the algorithm are-

1. Every user generates a pair of keys to be used for the encryption and decryption of messages.

2. One of the two keys is placed in a public register or some accessible file called as public key. The enduring key is kept private. As stated in Fig. 1 and Fig. 2, each user maintains a collection of public keys obtained from other users.

3. When Bob wants to send a confidential message to Alice, he encrypts the message using the public key of Alice.

4. When Alice receives the message, she decrypts it using her private key. None other than Alice can decrypt the message because she only knows her private key. This approach has access to public keys for all participants, and private keys are generated locally by each user and therefore need never be distributed. Provided that a user's private key remains protected and secured, arriving communication is secure. A system can change at any time its private key and publish the buddy public key to replace its old public key.

Fig. 6 summarizes the RSA algorithm.

The ingredients of RSA scheme involves key generation, encryption and decryption are as shown in following Tables I and II.

TABLE I. KEY GENERATION

Select p, q	p and q both prime, $p^1 q$
Calculate $n = p \times q$	--
Calculate $j(n) = (p-1)(q-1)$	--
Select integer e	$gcd\left(j(n), e\right) = 1; 1 < e < j(n)$
Calculate d	$d = e^{-1}\left(mod j(n)\right)$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

TABLE II. KEY GENERATION

Encryption	
Plaintext	$M < n$
Ciphertext	$C = M^e \bmod n$
Decryption	
Ciphertext	C
Plaintext	$M = C^d \bmod n$

IV. LAND MOBILE SATELLITE CHANNEL

Use Signal travelling in wireless media may be subjected to reflection, diffraction, shadowing and scattering as well as its power alter due to channel response.

If the power of signals fluctuates significantly under this situation, channel is said to be faded channel [10].

Fading can be defined as;

- Modulated signal subjected to deviation of attenuation while propagated through wireless channel due to response of channel.
- Unpredictable, irregular and random change in magnitude and phase.
- Fading is result of different reasons, Multi path fading, interference, shadowing, path loss etc.

Fig. 7 below depicts a typical mobile radio propagation scenario.

In presence of shadowing and multipath fading, the Quality of Service (QoS) and spectral efficiency over LMS channel drops significantly. In order to investigate

the transmission via multiple satellites it is indispensible to know the properties of the LMS channel [11].

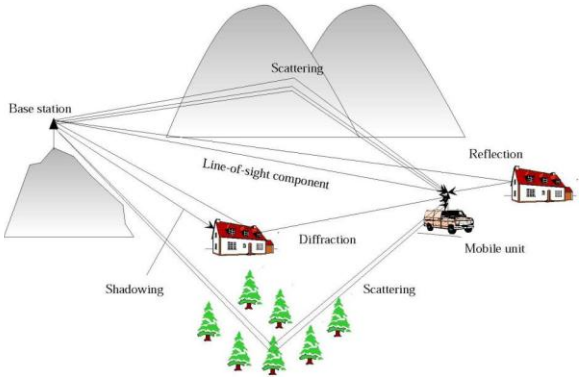

Figure 7. A typical mobile radio propagation scenario

In order to provide global coverage with a high signal quality to various users, seamless integration of terrestrial and satellites networks are likely to play a vital role in the forthcoming era of mobile communications [12].

In mobile channel modeling, we begin from fundamental channel models which are Rayleigh and Rice models. Thus, these two latter are the result of the sum of two Gaussian processes as shown in Fig 8.

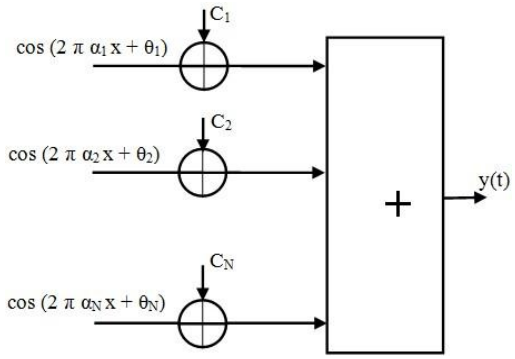

Figure 8. An example of sum-of-sinusoids principle

Frequency hopping (FH) techniques are used in the Global System for Mobile (GSM) communication system. Principle of frequency hopping in GSM is that the carrier frequency changes with every time division multiple accesses. A channel simulator that models accurately the physical model statistics determined by the frequency partition between two carriers in FH systems called a FH channel simulator. Such a simulator is important for the design, optimization and performance evaluation of wireless communications. Frequency hopping combined with error protection techniques and interleaving plays a very important role in combating fading in mobile radio communication channels. In Fig. 9 and Fig. 10, the simulation envelops with and without frequency hopping are shown [13].

Mainly, most of the channel model simulators are implemented based on the sum-of-sinusoids principle which is first introduced by Rice and then developed later. Starting from the idea that each signal can be expressed under sum-of-sinusoids, we assumed that any model type is able to be implemented following the sum-of-sinusoids principle [14].

In mobile channel modeling, we begin from fundamental channel models which are Rayleigh and Rice models. Thus, these two latter are the result of the sum of two Gaussian processes.

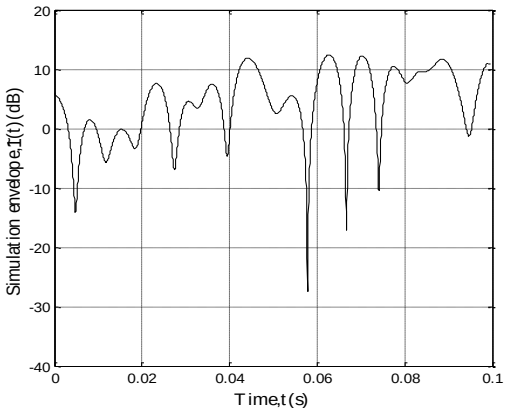

Figure 9. Simulation envelop without frequency hopping

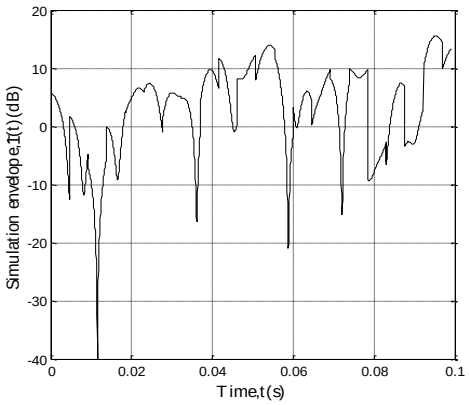

Figure 10. Simulation envelop with frequency hopping

V. Crypto-Coding

Crypto-coding is the single step technique where the two primitives such as error correction coding and encryption functionalities are brought together. This is as shown in Fig. 11.

In what follows we briefly discuss the cryptcoding system of McEliece from 1978, and the Kak's proposal from 1983 [15].

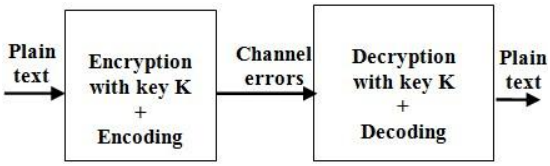

Figure 11. Crypto-encoding principle

A significance of the above requirements is that crypto-coding is different than traditional composition of encryption-then-encoding. Our assessment to introduce the new term crypto-coding is justified with the ability of this approach to accomplish both, the functions of secure encryption and error-correction in a single logical operation, exactly as described by the two conditions below [16].

A crypto-coding is a method that performs both, the functions of encryption and error-correction coding as a single primitive. It has a pair of algorithmic functions like (E,D) where E is called encrypt-coding algorithm and D is called decrypt-coding algorithm. (E,D) Satisfy the following conditions:

- Encryption (E,D) is a secure encryption scheme, which means it satisfies the correctness and the security conditions.
- Encoding (E,D) is an error-correction scheme and satisfies the coding condition also [17].

In cryptcoding if we use E and D to denote the encrypt-coding and decrypt-coding algorithm, respectively, the cryptcoding is realized in following two steps:

- $E(K,M)=C$ Encrypt-coding step in which an error resistant ciphertext C is created using the encryption key K.
- $D(K,C)=M$ Decrypt-coding step in which the original message ***M*** is restored from the erroneous ciphertext ***C*** after transmission (Hamming - $C,C^{'} \le t$).

We introduced a new type of Encryption and Error Correction scheme which is called "A Combined Encryption and Error Correction Scheme: RSA-Turbo". This combined system is presented in Fig. 12 and Fig. 13.

This Combined system will help in manufacturing Monoblocks in a single step [18].

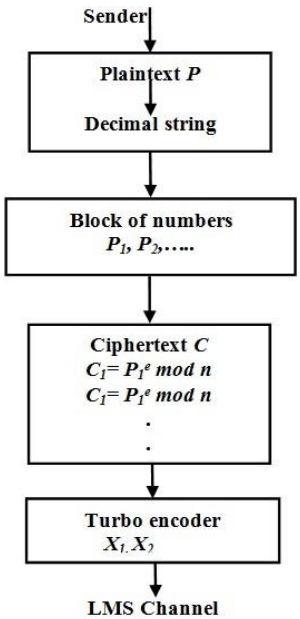

Figure 12. Crypto-encoding principle

In the transmitter part of the system, turbo encoder block is embedded in RSA encryption block. Encrypt-encoded message when transmitted through land mobile satellite channel, due to fading information gets corrupted. Then secured message is encoded initially using convolutional technique. Here the redundancy is added to detect and correct the errors introduced by the channel.

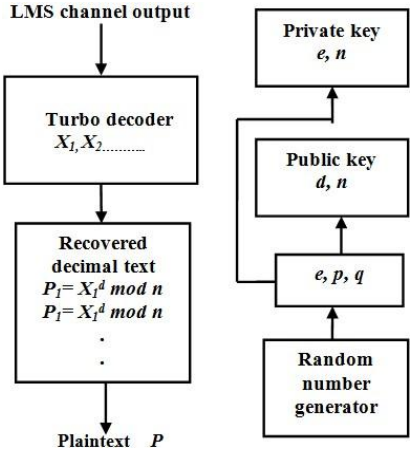

Figure 13. Crypto-decoding principle with key generation

In the receiver part of the system, the Viterbi decoding technique is combined with RSA decryption as decrypt-decoding where message gets channelized with correction [19]. The same experiment is performed using turbo codec for the better performance which has been investigated in results and discussions.

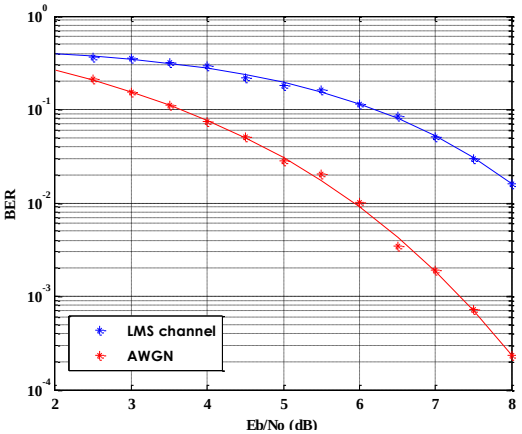

Figure 14. BER Performance of RSA-Convolution over LMS and AWGN Channels

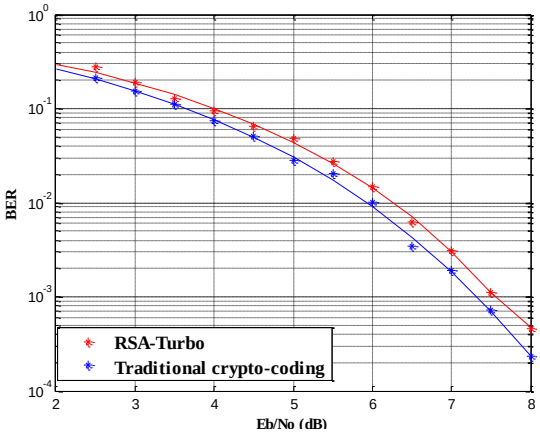

Figure 15. BER Performance of RSA-Turbo over LMS Channel

VI. Experimental Results

The bit error rate performance of overall Crypto-Coding system is compared with conventional Crypto-

Coding over Additive White Gaussian Noise (AWGN) and Land Mobile Satellite (LMS) channels.

The performance analysis found almost similar for both the types of channels when turbo coding is considered.

Fig. 14 demonstrates AWGN and LMS channel performances for RSA-Convolutional technique. At the decoder side Viterbi is used for error correction, it fails because of bursty noise. The AWGN shows better performance over LMS channel.

Fig. 15 shows the conventional crypto-coding and crypto-coding are examined for turbo code with interleaver. Here transmitter part includes iterative turbo encoder and receiver part BCJR technique. Both performances with BCJR turbo decoding algorithm are found approximately same.

The traditional crypto-coding and crypto-coding as a single step are simulated for 8 iterations. The results are found as shown in Fig. 16. The BER performance is improved to almost $\boldsymbol{10^{-7}}$**.** As the number of iterations increases performance shows better. In this case also turbo encoding with interleaver and decoding with BCJR is used.

The BER performance of Crypto-Coding as a single step is compared for different interleavers. However, RSA-Turbo demonstrates enhanced performance with S-random interleaver after eight iterations [20]. Fig. 17 gives the result of the same.

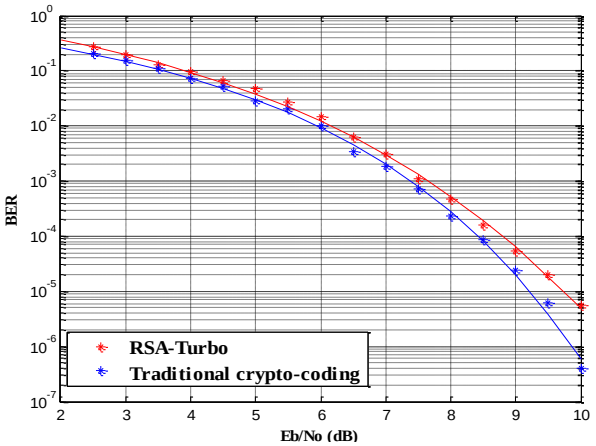

Figure 16. BER Performance of RSA-Turbo over LMS Channel

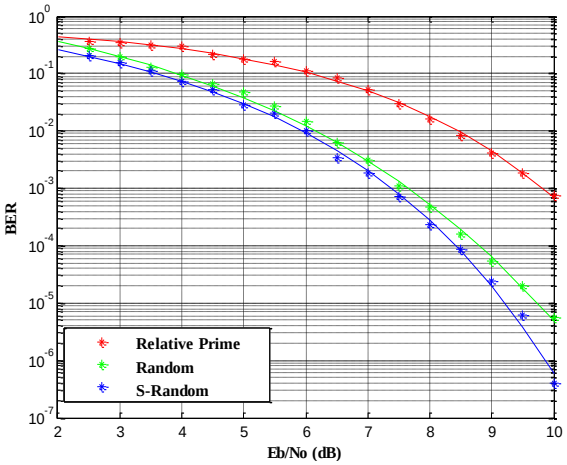

Figure 17. BER Performance of RSA-Turbo over LMS Channel with different interleavers

VII. Conclusion

In this paper, we instigate the concept of an improved combined cryptography-error correction method, which is called "Crypto-Coding as a single primitive". Primarily, the RSA is combined using convolutional code and demonstrated. But as Viterbi for decoding does not produce expected results because of bursty noise of channel. The algorithm called RSA-Turbo is developed and investigated on land mobile satellite channel. Also it is examined for three different interleavers for more than eight iterations and hence results are demonstrated. This modification is devised to enhance the efficacy of the system.

References

[1] A. Moghadam and V. T. Vakili, "Enhanced secure error correction code schemes in time reversal UWB systems," *Wireless Personal Communications*, vol. 64, no. 2, pp. 403-423, May 2012,

[2] H. Kaneko and E. Fujiwara, "Joint source-cryptographic-channel coding based on linear block codes," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science*, vol. 4851, pp. 158-167, 2007.

[3] Y. Jiang, *A Practical Guide to Error-Control Coding Using MATLAB®*, Artech House, 2010.

[4] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, 1948.

[5] M. Viterbi. (1998). Shannon theory concatenated codes and turbo coding. [Online]. Available: http:// oocs.donvblack.com/viterbi/index.html

[6] S. Lin and D. J. Castello, "Convolutional code," in *Error Control Coding—Fundamentals and Application*, NJ: Prentice-Hall, 2004, ch. 11, sec. 11.2, pp. 485-510.

[7] K. Sripimanwat, "Turbo code applications a journey from a paper to realization," *National Electronics and Computer Technology Center (NECTEC)*, 2005.

[8] J. Pelzl, *et al.*, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.

[9] M. Patzold, *Mobile Radio Channels*, John Wiley & Sons, 2011.

[10] W. Li, V. K. Dubey, and C. L. Law, "The performance of turbo coding over power-controlled fading channel in ka-band LEO satellite systems," *IEEE Trans. on Vehicular Technology*, vol. 52, no. 4, pp. 1032-1043, Jul. 2003.

[11] Y. Li and X. huang, "The simulation of independent Rayleigh faders," *IEEE Trans. on Commun.*, vol. 50, no. 9, pp. 1503-1514, Sep. 2002.

[12] J. A. Heller and I. M. Jacobs, "Viterbi decoding for satellite and space communication," *IEEE Trans. Comm. Tech.*, vol. 19, no. 5, pp. 835-848. Oct. 1971.

[13] M. Murroni, "Robust transmission of compressed streams over land mobile satellite channel at ku-band," in *Proc. IEEE Vehicular Technology Conference*, 2008, pp. 2917-2921.

[14] Payandeh, M. Ahmadian, and M.R. Aref, "An adaptive secure channel coding scheme for data transmission over LEO satellite channels," *Journal of Scientia Iranica*, vol. 13, no. 4, pp. 373-378, Oct. 2006.

[15] S. C. KAK, "Encryption and error-correction coding using D sequences," *IEEE Trans. Computer communications*, vol. 34, no. 9, pp. 803-809, Sep. 1985.

[16] Gligoroski, S. J. Knapskog, and S. Andova, "Crypto-Coding - Encryption and error-correction coding in a single step," in *Proc. International Conference on Security and Management*, Jun. 2006.

[17] S. J. Knapskog, "New cryptographic primitives (plenary lecture)," in *Proc. IEEE 7th Computer Information Systems and Industrial Management Applications*, 2008, pp. 3-7.

[18] H. C. Volkan, O. Osman, and N. UCAN, "A combined encryption and error correction scheme: AES-Turbo," *Journal of Electrical and Electronics Engineering*, vol. 9, no. 1, pp. 891-896, 2009.

[19] N. Zivic and C. Ruland, "Parallel joint channel coding and cryptography," *International Journal of Electrical, Computer, and Systems Engineering*, pp. 140-144, 2010.

[20] N. Zivic and C. Ruland: "Channel coding as a cryptography enhancer," *WSEAS Transactions on Communications*, vol. 7, Mar. 2008.

Rajashri Khanai is perusing PhD in the area of error correction coding and cryptography for wireless communication. She is currently Assistant Professor in the department of Electronics and Communication Engineering, Jain College of Engineering, Belgaum, Karnataka, India. Her research interests include cryptography, error correction coding, neural networks applied to wireless communications.

Dr. G. H. Kulkarni received his PhD from JNTU, Hyderabad, India in electrical engineering. He is presently Professor and Head, Department of Electrical and Electronics Engineering, Jain College of Engineering, Belgaum. His research interests include electrical power systems, neural networks applied to electrical engineering.

Dattaprasad A. Torse is a research scholar of VTU, Belgaum, Karnataka, India. He is currently perusing PhD in the area of biomedical signal processing. He is assistant professor in the department of electronics and communication engineering, Gogte Institute of Technology, Belgaum, Karnataka, India. His research interests are biomedical signal processing and wireless communication systems.