Low Complex Crypto based Channel Coding with Turbo Code

Celine Mary Stuart
Department of Electronics and Communication Engineering, National Institute of Technology
Calicut-673601, Kerala, India

Nandan S.
Department of Electronics and Communication Engineering, National Institute of Technology
Calicut-673601, Kerala, India

Deepthi P.P.
Department of Electronics and Communication Engineering, National Institute of Technology
Calicut-673601, Kerala, India

ABSTRACT
A novel encryption system to increase security in a three tier manner without any additional complexity is proposed in this paper. The encryption block here is a Shrinking generator which is a Linear Feedback Shift Register (LFSR) based stream cipher system in which controlled randomness provides security. The channel coding technique used is Turbo code that performs very well and provides results near Shannon's Limit. The design of interleaver used in turbo code provides security while channel coding. Puncturing pattern designed for channel coding further increases the security of the system and improves the code rate also. Security of the system is achieved by hiding the keys used in code generation and puncturing from unintended users. For an intended user, performance of the channel coding system is further improved by using Soft Input Decryption (SID) technique. The hardware complexity of the proposed Shrinking Generator Based Cipher (SGBC) is compared with joint coding cryptographic schemes available in literature. Improved Linear Consistency Attack is mounted to analyze the security of the proposed system and the results show that a significant increase in security could be achieved without any additional increase in complexity.

Keywords
Turbo code, Puncturing, Soft Input Decryption, Improved Linear Consistency Attack

1. INTRODUCTION
With the advance of wireless communication technology, mobile communications have become more convenient than ever. However, due to the openness of wireless communication, it is difficult to protect the privacy between communicating parties. Also most of the communication devices are becoming more portable and are constrained in resources such as battery power and computational power. Hence, there is a great need to provide good security without much increase in computational or hardware complexity in a secure communication system. Research is going on to improve security through channel coding without increasing computational / hardware complexity.

With the emergence of resource constraint wireless devices and adhoc network, encryption at higher layer becomes difficult to implement. As a result, there has been a lot of interest in implementing encryption at the physical layer. An existing efficient method of physical layer encryption is Error Correction based Cipher (ECBC) [1].

Error correction coding techniques are used to ensure reliable delivery of digital data over unreliable communication channels. Turbo code [2] is a promising error correcting code which gives performance near to Shannon's limit.

In Turbo code, encoder contains two Recursive Systematic Convolutional (RSC) coders. The systematic data stream input is shuffled through an interleaver and given to second RSC coder. Research has shown that pseudo random interleaver can provide good code performance for Turbo code [3-5]. Soft decision decoding makes use of 'turbo' concepts which needs the knowledge of structure of interleaver for successive iterations. If the structure of interleaver is known only to trusted users, decoder performance will be deteriorated by a great amount for an attacker. This allows introducing an additional level of security.

Puncturing [6-9] is the process of deleting some parity bits from the codeword according to a puncturing pattern which is known only by the trusted users. This is done to adjust the code rate to improve bandwidth efficiency and can also be used to improve security.

Soft Input Decryption [10-12] is a method for improving the performance of channel coding using cryptographic techniques. Soft Input Decryption (SID) is a novel method which uses L-values (soft output) of a Soft Input Soft Output (SISO) channel decoder for the correction of input data of SID blocks which have been modified during the transmission over a noisy channel. Hash code for integrity verification of data is used here for improving result of channel coding.

Attempts are made to explore methods for introducing security in channel coding with low or no additional computational complexity. Also, the increased security of the so designed crypto systems is quantified in terms of time taken to attack the system.

The remainder of the paper is organized as follows: In section 2, the basics of LFSR based stream cipher and attack mounted are explained. In section 3, the basic concepts of Turbo code, Puncturing and Soft Input Decryption are discussed. Section 4 explains the proposed Shrinking Generator Based Cipher while section 5 discusses the simulation results and security analysis of proposed channel coder.

2. STREAM CIPHER
Stream ciphers are developed as an approximation to the properties of Shannon's analysis of the completely secure cryptosystem known as the one-time pad. The drawback of such a scheme is that the key stream should be as large as the

message stream. This motivates the design of stream ciphers using a small secret key that pseudo randomly generate a very long key stream sequence. Such systems are not unconditionally secure but are computationally secure. The design criteria for key stream generators are large period and good statistical properties of the key stream sequence. For some sequences like the LFSR sequences, one can establish the long term statistical properties. They are measured as frequency distribution of certain patterns on a period which should be close to the expected value for a purely random sequence. The security would depend upon the randomness of the key stream which depends on the unpredictability and balanced distribution of the key stream bits.

2.1 LFSR based stream ciphers

The vast majority of modern stream ciphers use one or several linear feedback shift registers as building blocks. The main reasons for the popularity of LFSR based ciphers are that they have large period, good statistical properties, are conveniently analyzed using the algebra over finite fields, and can be implemented fast in both hardware and software. As the initial seed of an LFSR is easy to predict in a known-plaintext attack, the linearity properties must be destroyed in a stream cipher design. This is achieved by introducing nonlinearity in the system. There are two main methodologies to achieve non linearity. They are either using non linear Boolean function or to clock irregularly. In our work, irregular clocking based Shrinking Generator is used, where the output sequence can be controlled by secret keys to provide security while encoding.

2.1.1 Shrinking generator

Coppersmith et al [13] first presented a design of the Shrinking generator. Shrinking generator is a Linear Feedback Shift Register based stream cipher [14]. It is based on two Linear Feedback Shift Registers (LFSR)'s, S (selector), and the A (data) registers as shown in figure 1. The A sequence, generates output bits, while the S sequence, controls their output. Both A and S are clocked. If the S bit is 1, then the A bit is output; if the S bit is 0, then A bit is discarded, nothing is output, and we clock the registers again. Shrinking generator has good random like properties that exist in LFSR's, and also another important property that does not present in LFSR sequences, such as the Exponential Linear Complexity. Period of the key stream (z-sequence) is exponential in both the lengths of the A and the S sequences.
Conditions that must be satisfied in a secure design are
(1) The periods of the two LFSR's - L_S and L_A must be coprime. i.e. gcd $(L_S, L_A) = 1$
(2) Use of maximum length LFSR's for the LFSR A and S in the shrinking generator.
Main properties of the Shrinking Generator are
(1) If gcd $(L_S, L_A) = 1$, then the output sequence, Z, has a period $(2^A\text{-}1)\ (2^{S-1})$ where A and S are the length of seeds of LFSR A and LFSR S respectively.
(2) The linear complexity $L(Z)$, of the output sequence Z, satisfies:
$L_A\ (2^{S-2}) < L\ (Z) \leq L_A\ (2^{S-1})$

2.2 Cryptanalytic attacks on LFSR based stream ciphers

Cryptanalytic attack involves techniques to break the cipher system by acquiring its key. The attack can be a *cipher text only attack* or a *known plain text attack* depending on the amount of information available to the cryptanalyser. Known plaintext attack is considered for analyzing the security of LFSR based stream ciphers. A system that is secure against known-plaintext attack can be considered to be secure against other possible attacks. When comparing attacks, two important measures considered are time complexity and data complexity. Time complexity gives a measure of the number of computations required to be performed to carry out the attack. Time complexity can be obtained by the CPU time taken for successfully completing the attack. Data complexity of an attack is specified by the number of key stream bits required to be known to mount the attack successfully.

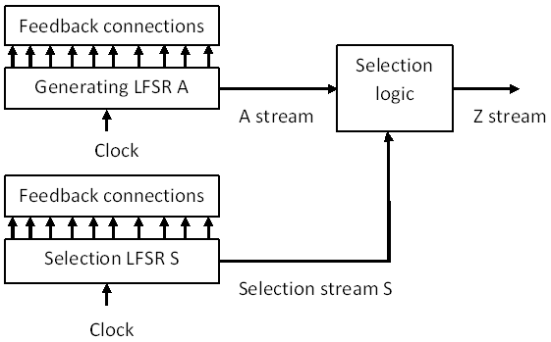

Figure 1: Shrinking Generator

2.2.1 Improved Linear Consistency Attack

The attacks for clock controlled generators available on the literature are based on the exhaustive key search on the initial state of control register or generating register. *Improved linear consistency attack* [15] works well for shrinking generator (SG). The attack starts with applying a brute force selection on the initial state of control register. Then by utilizing the linearity present in the generating registers, an analysis is done to check the validity of the existence of selected initial state of control register. After that, initial state of generating register is retrieved. Following factors are known to the attacker:
1. N bits of key stream $Z = (Z_1, Z_2, \ldots Z_N)$
2. Feedback polynomials of both LFSRs.
Steps involved:
1. From the generator polynomial of A, derive a low weight cyclic equation λ.
2. Consider LFSR-S: $x^3 + x + 1$ and LFSR-A: $x^3 + x^2 + 1$.
3. General linear recursion equation for LFSR with state bits $a_2\, a_1\, a_0$ and feedback polynomial $q_0 + q_1\, x + q_2\, x^2 + q_3\, x^3$ is $a_3\ q_0 + a_2\, q_1 + a_1\, q_2 + a_0\, q_3 = 0$. For LFSR A, $a_0 = a_1 + a_3$ or $a_3 = a_1 + a_0$ and $a_4 = a_2 + a_1$. In general, $a_n = a_{n-2} + a_{n-3}$

3. TURBO CODE

3.1 Basic Concepts

The fundamental turbo code encoder shown in figure 2 is built using two identical recursive systematic convolution (RSC) encoders with parallel concatenation. The interleaver plays a very important part in the construction of good Turbo codes [4]. The classical use of interleaver is to randomize the location of errors, enabling the use of random-error-correcting codes on channels with burst error patterns. The random interleaver uses a fixed random permutation and maps the input sequence according to the permutation order. The basic feature of Turbo code is its encoding simplicity.

Decoding of Turbo code is done through maximum a posteriori (MAP) algorithm. On receiving a corrupted code bit sequence, the process of decision making with a posteriori

probabilities (APPs), allows the MAP algorithm to determine the most likely information bit sequence transmitted at each bit time. Turbo code has become a very promising code for future communication systems, due to the very good performance of the decoder.

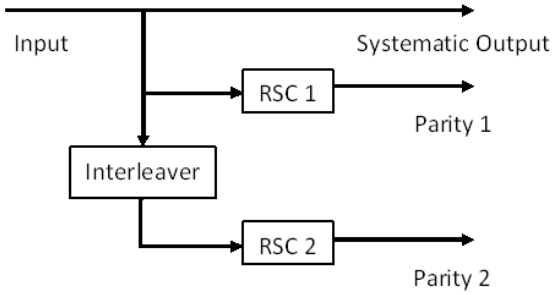

Figure 2: Basic Turbo encoder

3.2 Puncturing of Turbo codes

Puncturing is the process of deleting some parity bits from the codeword according to a puncturing pattern. To achieve unequal error protection, parallel concatenated convolutional codes (PCCC) with two identical constituent encoders with a variable rate of 1/2 to 1/3 using the same mother encoder, the Rate Compatible Punctured Turbo Code (RCPTC) [8] is introduced. The specification of an RCPTC consists in finding suitable mother encoder(s), the interleaver(s), and the puncturing patterns to obtain the desired code rate range. PCCC with rate 1/3 is selected as mother code. The design methodology includes the following three consecutive steps. The first step is the selection of constituent encoders having good performance at low signal-to noise ratio with particular attention to decoding complexity. The second step is the design of turbo-code interleaver which is based on the codeword weight distribution and on the achievable performance on the Additive White Gaussian Noise (AWGN) channel, using a maximum likelihood approach. The third step is to select puncturing schemes based on both the weight distribution and the achievable performance on the AWGN channel.

Kousa et al. [9] proposed the puncturing scheme with the codeword weight calculation so that performance is not much affected. To obtain a code rate of k/(k + 1), one parity bit only is transmitted for every k information bits presented to the encoder input. The rates of the two constituent encoders after puncturing are assumed to be the same and the parity bits to be transmitted alternate between the two encoders. Therefore, for every 2k input bits, only two parity bits are transmitted by the puncturing scheme, one from each of the two constituent encoders.

3.3 Soft Input Decryption

Soft Input Decryption [10-12] is a method for improving the performance of channel coding using cryptographic techniques. The method is based on the combination of cryptography and channel coding, wherein the cryptographic checksum called hash is used to improve the performance of channel coding. Cyclic Redundancy Check (CRC) hash function is used for generating the hash value and is appended to message for data integrity verification. The cryptographic CRC hash function h(M) is defined as: $M(x)\ x^n \bmod g(x)$, g(x) is the irreducible polynomial of degree n over GF(2), where n is the hash value size in bits. M is the message to be hashed and M(x) is the message polynomial with degree 'm–1', where 'm' is the message size. x^n is the multiplication factor. The operation of division modulo a polynomial over GF (2) is implemented through a simple LFSR with taps or connections determined by the division polynomial.

Figure 3 shows the algorithm of Soft Input Decryption.

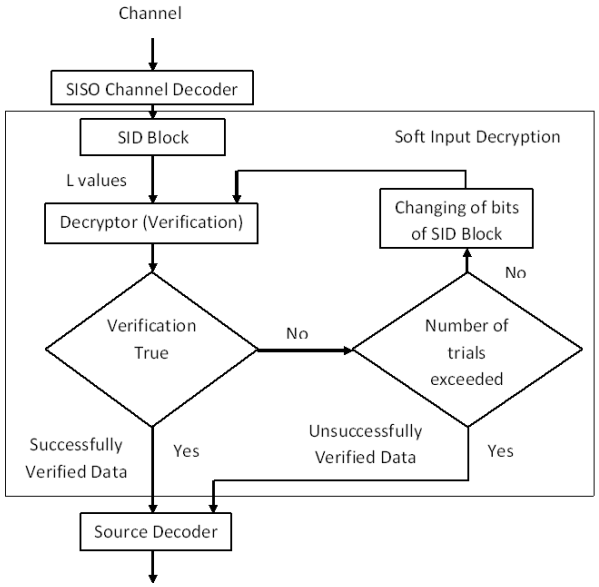

Figure 3: Algorithm of Soft Input Decryption

4. PROPOSED SHRINKING GENERATOR BASED CIPHER TO INCREASE SECURITY

In the present scenario of wireless communication, security of a secure communication system is only due to the encryptor, where complex design methods are employed to incorporate security. But we can increase the security of the system by introducing secrecy in the channel coder also. The proposed Shrinking Generator Based Cipher (SGBC) is implemented by including a key controlled Shrinking Generator as encryption block prior to the crypto based channel encoder block. The channel encoder block is implemented using Turbo code.

4.1 Proposed Crypto based Turbo Code

4.1.1 Introducing security in Turbo code with key controlled interleaver

For embedding security in Turbo coding, a keyed secrecy has to be introduced in the interleaver design [16]. Hence we go for the design of pseudo random inter-leavers made of shift registers. Since the interleaving pattern is known only to the intended user, decoding is possible only for trusted users. For un-intended users, any guess on the channel code structure (interleaver) help to retrieve only an approximate version of key stream in known plaintext attack. This makes decoding difficult for an un-intended user.

In a secure interleaver design where the inter leaved positions are determined by the key, an attacker will not be able to implement this efficient decoding due to lack of knowledge of the key. In a known plaintext attack on stream cipher, the retrieved key stream is obtained by xoring known plaintext with cipher text at the output of the channel decoder. When the channel decoder [17] performance is poor, the retrieved key stream will also vary from actual key stream to a great extent. This will cause a decrease in correlation between a

linear version of LFSR output and key stream, thereby increasing attack complexity. Thus for an intruder an additional level of security is achieved by reduced performance of channel decoder without any additional increase in complexity.

4.1.2 Increasing security of key controlled Turbo code using puncturing

Security of the system is increased by introducing puncturing in the channel coder [6-8]. Figure 4 shows the key controlled Turbo encoder using puncturing. The puncturing pattern is made available only for the intended users. So the unintended users should have to go for a brute force search of the puncturing pattern, which increases the security of the system. The redundant bits in coding decrease the bandwidth efficiency. Puncturing is the tradeoff between rate (bandwidth efficiency) and performance. Puncturing increases code rate without increasing complexity and decreases free distance of code, to some extent. If puncturing pattern is properly designed, improvement in terms of rate can be achieved without much sacrifice on error correction capability. Although punctured turbo code could increase bandwidth efficiency, different punctured locations could give different performance at the receiver. When the bit in codeword is with a high weight, it is required to avoid puncturing that bit. Hence it is not possible to puncture the systematic sequence because the systematic bit is with a high weight. Consequently, the puncturing scheme should choose the lower weight bits to be punctured.

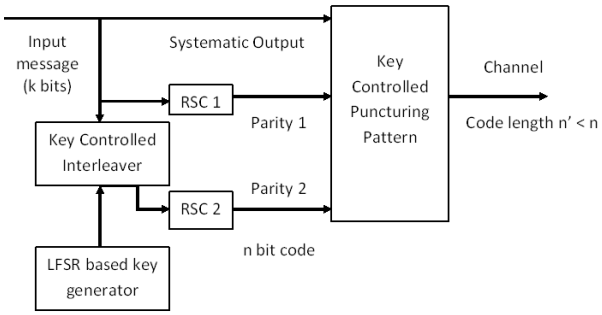

Figure 4: Key controlled Turbo encoder using puncturing

4.2 Improvement of performance of proposed crypto based Turbo coder using Soft Input Decryption

If the data is tampered on transmission, at the receiver side, verification of generated hash with extracted hash fails. But if there is a small variation in data due to channel noise, data integrity verification should not fail. Rather, the data can be corrected to provide proper hash verification, provided the variation in data is within limits of channel noise error. The data values that can be corrected for proper verification, is decided by L values of data, which give indication about reliability in decoding.

The results of the tested performance of L-values show how many L-values are necessary for the correction of SID blocks. The number of L-values is estimated for different lengths of SID blocks as well as for different Eb/No ratios. The cryptographic CRC hash generated and transmitted along with the information sequence improved the performance of channel coder. The decoding technique used for Turbo code is Maximum A-Posteriori (MAP) algorithm.

5. EXPERIMENTAL RESULTS

5.1 BER plot of proposed Turbo coded system with key controlled interleaver

The BER Performance of proposed Turbo coded system with key controlled interleaver for intended and un-intended users is shown in figure 5. The upper plot is obtained for an unintended user who does not know the key used for the design of the interleaver of turbo code. Since the data is completely unknown, the error rate is very high. The second plot is for uncoded turbo code, whose BER performance is also very poor. The third plot gives the performance of proposed turbo code after a single iteration for an intended user who knows the key. When the number of iteration is increased, the performance is also increased as shown by the bottom plot.

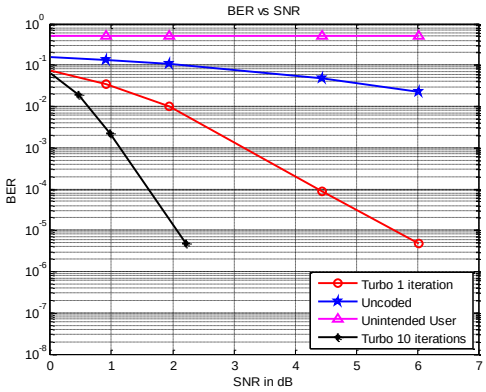

Figure 5: BER Performance of proposed Turbo coded system for intended user and un-intended users with unknown interleaver

5.2 BER plot of proposed key controlled Turbo code with puncturing

The BER performance of proposed Turbo code for an intended user who knows interleaver and puncturing pattern is shown in figure 6. For a conventional Turbo coder with rate 1/3, the error performance of proposed system is better. As the rate increases the performance of the system degrades.

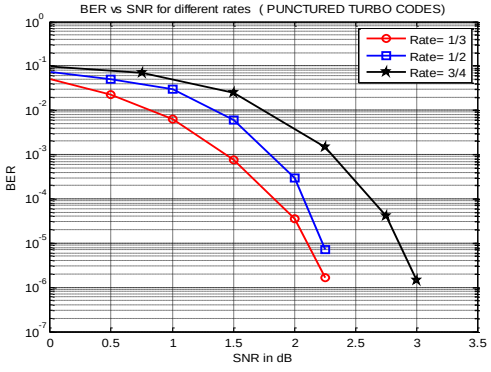

Figure 6: BER performance of proposed key controlled Turbo code with puncturing

5.3 BER plot showing the performance of proposed crypto based Turbo code using Soft Input Decryption

Soft Input Decryption is done on proposed crypto based Turbo code for getting an improvement in the coding gain. A punctured Turbo code with rate =3/4 is considered here. Figure 7 shows the performance improvement of proposed crypto based Turbo code as the number of |L|-values increases.

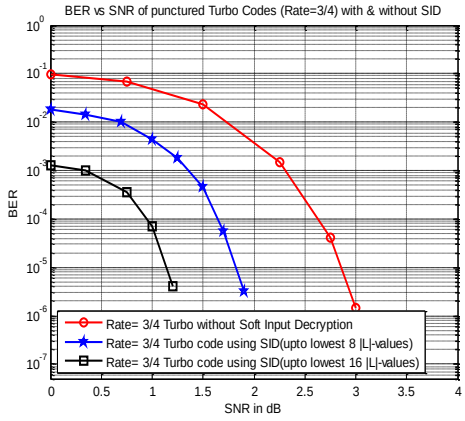

Figure 7: BER performance of proposed crypto based Turbo code using Soft Input Decryption

5.4 Security Analysis of Crypto based Turbo coded system

The improved linear consistency attack is mounted on crypto based Turbo coded system and the security is measured in terms of time of attack. Puncturing the channel coded bits will result in increasing the security of the system. The attack is done with both unknown interleaver and unknown puncturing pattern. Table 1 shows the result obtained by mounting attack on Turbo coded system with and without security in channel coding.

Length of Key	Time to attack Turbo coded system without security in channel coding (seconds)	Time to attack Un-punctured Turbo Coded system with Unknown Interleaver (seconds)	Time to attack Punctured Turbo Coded system with Unknown Interleaver and Unknown Puncturing pattern (seconds)
6	0.5386	1674.5739	3026.7443
7	1.4558	3520.3926	7821.9032
8	3.3135	15338.7372	26284.1842
9	20.622	Very high	Very high

Table 1: Security Analysis of Punctured Turbo coded system

Time required to attack a system without security is very small while the time increases if the interleaver is unknown to the attacker. If the puncturing pattern is also unknown to the attacker, attack time increases further. It is found that the attack time increases exponentially with the length of the key.

6. CONCLUSION

A novel method to increase the security of a communication system without increasing the hardware complexity is proposed in this work. For improved security, cryptographic operations are embedded into channel coding. By hiding the keys used in code generation and puncturing from unintended users, the proposed system gains additional security over a normal stream cipher based system. For the resource limited devices, the proposed SGBC provides a very good alternative to implement a highly secure stream cipher based system without any additional increase in complexity. For increasing the coding gain of the proposed low complex crypto based channel coded system, Soft Input Decryption is done, which uses cryptographic hash values for data verification. Thus present work reveals that channel coding can be used for the improvement of results in crypto system or cryptography can be used to improve results in channel coding.

7. REFERENCES

[1] OluwayomiAdamo, M. R. Varanasi, “Joint Scheme for Physical Layer Error Correction and Security”, International Scholarly Research Network, ISRN Communications and Networking, Volume 2011, Article ID 502987, 9 pages.

[2] Berrou. C., Glavieux. A and Thitimajshima. P, ‘Near Shannon limit error-correcting coding: turbo codes’. Proc. IEEE International Conference on Communications, Geneva, Switzerland, 1993, pp.1064–1070.

[3] J. Hokfelt, O. Edfors, and T. Maseng,”A Turbo Code Interleaver Design Criterion Based on the Performance of Iterative Decoding”, IEEE Communications Letters, Vol. 5, No.2, February 2001.

[4] KashifNizam Khan, JinatRehana, RameswarDebnath, “An Improved Interleaver Design for Turbo Codes”, International Conference on Information and Communication Technology ICICT 2007, 7-9 March 2007.

[5] S. Lin, D. J. Costello, Error Control Coding: Fundamentals and Applications, Prentice Hall, Englewood Cliffs, N.J., 1983.

[6] J. Hagenauer, “Rate compatible punctured convolutional codes and their applications," IEEE Transactions on Communications, vol. 36, no. 4, pp. 389-400, Apr. 1988.

[7] M. Fan, S. C. Kwatra, and K. Junghwan, “Analysis of puncturing pattern for high rate turbo codes," in Proc. of Military Communication Conference (MILCOM'99), NewJersey, USA, Oct. 1999, pp. 547-550.

[8] F. Babich, G. Montorsi, and F. Vatta, “Design of rate-compatible punctured Turbo (RCPT) codes," in Proc. International Conference on Communication (ICC'02), New York, USA, Apr. 2002, pp. 1701-1705.

[9] M.A. Kousa and A.H. Mugaibel, “Puncturing effects on Turbo Codes,” IEE Proceedings on Communications, Vol.149, 2002, pp.132-138.

[10] N. Živić, C. Ruland, ”Channel Coding as a Cryptography Enhancer”, Advances in Communications, Proceeding in the 11th WSEAS International conference on Communications (part of the 2007 CSCC multiconference), AgiosNikolaos, Crete Island, Greece, July 26-28, 2007.

[11] NatasaZivic, "Strategies and Performances of Soft Input Decryption", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1 No.1, May 2009.

[12] NatasaZivic, "Iterative method for improvement of coding and Decryption", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009.

[13] Coppersmith, D., Krawczyk H., and Mansour, Y. (1994):"The Shrinking Generator", Proceedings of Crypto-93, LNCS Vol 773, Springer-Verlag, 1994, pp. 22-39.

[14] KANSO, A. (2003): Clock-controlled shrinking generator of feedback shift registers, Lecture Notes in Computer Science, vol. 2727, Springer Verlag: 443-451.

[15] H. Molland, "Improved Linear Consistency Attack on Irregular Clocked keystream Generators", Fast Software Encryption-FSE'2004, LNCS vol. 3017, Springer-Verlag, (2004), pp. 109-126.

[16] Qian Mao; Longii Sun; ChuanQin : "Joint Error Correction and Encryption Scheme Based on Turbo Codes", IEEE International Symposium Intelligence Information Processing and Trusted Computing (IPTC), Oct. 2010.

[17] Silvio A. Abrantes, "From BCJR to turbo decoding: MAP algorithms made easier © Silvio A. Abrantes, April 2004