International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Vol. 3, No. 4, October 2014

Research Paper

EMBEDDING SECRECY IN CHANNEL CODING USING LDPC CODES

B Yamini Pushpa[1]* and L Ashok[1]

*Corresponding Author: B Yamini Pushpa, ✉ yamini.pushpa@gmail.com

Over the Internet, various communications such as electronic mail or Web browsers are not secure for sending and receiving sensitive data. This made cryptographic methods to be known and used even by common-man in communication. Cryptography concerns the ways, in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping using channel codes, ciphers and other methods. The public key system eliminates the key distribution process that hampers all private key systems since there no need to communicate with secret keys among communicating parties. However, a problem that arises with this system is lack of assurance of the true identity of the required party and, associated complexity in operations is too large to be used in resource constrained devices. Hence in this work, methods to introduce security in channel coding without any additional complexity in operations and use of it together with symmetric key encryption systems are attempted. The channel coding method used in this work is Low Density Parity Check (LDPC) codes. Through insertion of security in channel codes it is possible to verify the error correction capability of LDPC codes and to quantify the increase in security of the overall communication system.

Keywords: Public key system, Stream ciphers, Construction of LDPC codes, Encoding and decoding methods of LDPC codes

INTRODUCTION

Cryptography concerns the ways, in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using channel codes, ciphers and other methods, so that only particular people can see the real message. Cryptography can be used for the improvement of channel decoding. This is known as Joint Channel Coding and Cryptography.

The noisy channel coding theorem of information theory proves that, if properly coded information is transmitted at a rate

[1] Madanapalli Institute of Technology and Management Science, Angallu (V), Madanapalle 517325, Chittoor District, AP, India.

below channel capacity, then the probability of decoding error can be made to zero. Channel coding uses redundant information for error correction that occurs during the data transfer over a noisy channel. In practical channel codes, which provide performance near Shannon limit are Turbo codes and Low Density Parity Check (LDPC) codes. The internet users may need secure communication to transmit and receive information. This made cryptographic methods to be known and used even by common men in communication. But in many of the communication applications such as RFID, smart cards, sensor networks, the communication systems are constrained in resources, especially in power. Hence there is a great demand to design and develop secure communication system of low computational/ hardware complexity.

One possible method to provide security is to embed secrecy in channel coding techniques. LDPC code, which are gaining increased popularity in recent times and provide near Shannon limit performance. The code generation methods for these codes make use of randomness. Hence there is a great scope for research in identifying methods to embed secrecy in the code generation methods. The degradation in the performance of decoder is due to lack of knowledge of secret key that is used in code generation.

Great amount of research is going on to develop efficient methods of generation for LDPC codes. Almost all methods make use of either random or semi-random techniques to generate parity check matrix H. Generator matrix G for code construction is obtained from H matrix. Decoding techniques require construction of H matrix at the receiver. Hence if the random or semi-random construction methods make use of a secret key, the receiver can get H matrix by knowing the secret key. Thus, the construction methods of LDPC codes allow security in communication system without additional complexity.

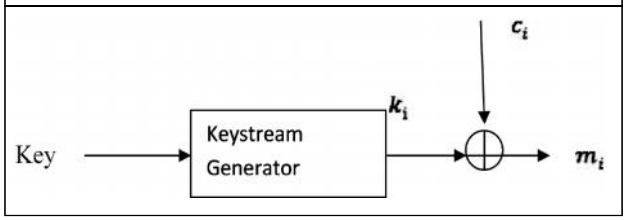
There are various methods for construction of low density parity check codes. Random construction of LDPC codes can be seen in Gallager (1962) and Mackay (1999) and tutorial paper (William Ryan, 2003). The encoding of LDPC codes can be done by using Gauss Jordan elimination to get the generator matrix in systematic form (William Ryan, 2003). The soft decision decoding algorithm for LDPC codes is message passing or belief propagation or sum-product algorithm (Enricopaolini *et al.*, 2003; Zongjie Tu and Shiyong Zhang, 2007; William Ryan, 2003; Daniel Castello Jr., 2009; and Bernhard Leiner, 2005). The various versions of sum-product algorithm are (i) sum-product algorithm in probability domain (ii) sum-product algorithm in logarithmic domain which reduces the multiplication complexity into additions. (i) Min-sum algorithm which is the approximation of (ii) reduces the additions by taking the minimum value.

ENCRYPTION USING STREAM CIPHERS

Stream ciphers have much lesser hardware complexity compares to their competent say block ciphers in symmetric key cryptosystems. This low hard ware complexity and real time operation of stream ciphers make them highly suitable for encryption in many of the present day communication systems. The heart of a

stream cipher is the key stream generator which produces pseudo random sequence. LFSRs as m-sequence generators are popular pseudo random sequence generators. LFSRs are used as key stream generators due to the easiness in hardware implementation. Although the implementation of LFSR is pretty low, the output sequence of the LFSR is easily predictable due to the linearity present between the bits in the sequence. So the LFSR as such is not preferred as a key stream in cryptosystem.

Figure 1: Encryption Using Stream Ciphers



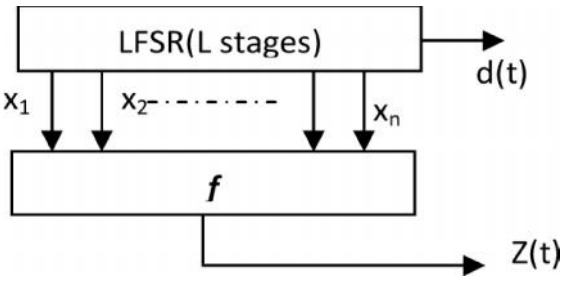
In order to make the cryptosystem secure, stream ciphers based on LFSR must break the inherent linearity. There are two ways to introduce non linearity in LFSR based stream ciphers are: (1) by irregularly clocking the LFSR and (2) by using non-linear Boolean function. The Non-Linear Filter Generator (NLFG) and non-linear combination generator fall under the first category and clock controlled generators such as shrinking generator, alternating step generator fall under second category.

Non-Linear Filter Generator

In the NLFG the keystream is generated by nonlinearly combining the outputs of different stages of LFSR using a non-linear Boolean function *f*, called the filter function. A Boolean function maps one or more binary input variables to a binary output variable. The keystream Z is given as $Z = f(x_1, x_2, \ldots, x_n)$, where $x_1, x_2, \ldots, x_n$ are the outputs of the different stages of the underlying maximal length LFSR. A Boolean function is characterized by its cryptographic properties like nonlinearity, balancedness, correlation probability and algebraic degree.

Randomness properties, statistical properties and cryptographic strength of the resulting keystream are dependent on the primitive characteristic of the feedback polynomial used and the properties of the nonlinear filter function *f*. To obtain keystream sequence having good statistical properties, the filtering function *f* should be balanced and the feedback polynomial of the LFSR should be chosen to be a primitive polynomial. Period of the resulting keystream is exactly same as that of the underlying LFSR, i.e., 2^L-1 or a divisor of 2^L-1, where L is the length of the LFSR. The linear complexity of $z(t)$ is less than or equal to $L_m = \sum_{i=1}^{m} \binom{L}{i}$, where m is the algebraic order of the nonlinear Boolean function.

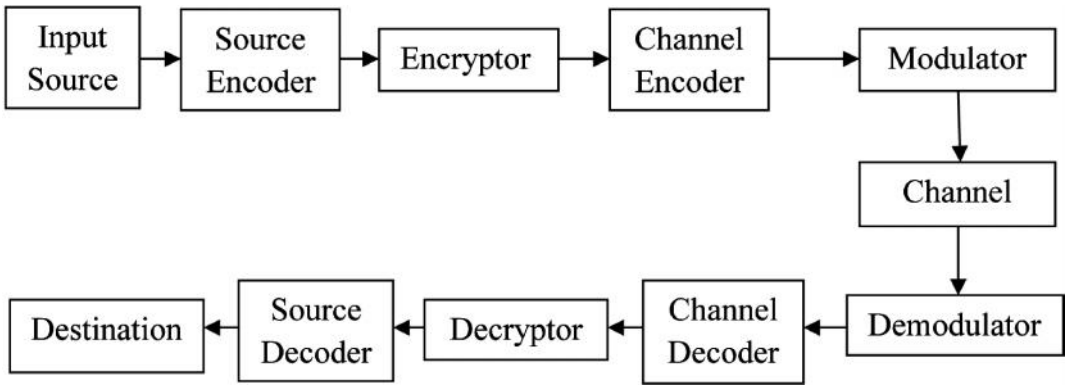
Figure 2: Nonlinear Filter Generator



EMBEDDING SECRECY IN CHANNEL CODING

The complete block diagram of a secure communication system is shown in Figure 3. The encryptor is placed after source-coding

Figure 3: Overall Communication System Block Diagram



since redundancy in data will help an attacker to break a secure system. But majority of modern communication systems in use today are constrained in resources such as battery power and computational power.

A method to combine channel coding with cryptography in such a way as to increase security for a given computational/ hardware complexity or to reduce complexity for a given security in a secure communication system is tried in this work. The degradation in the performance of decoder due to lack of knowledge of a secret key that is used in generation of channel code is used here to embed/increase the security of the communication system.

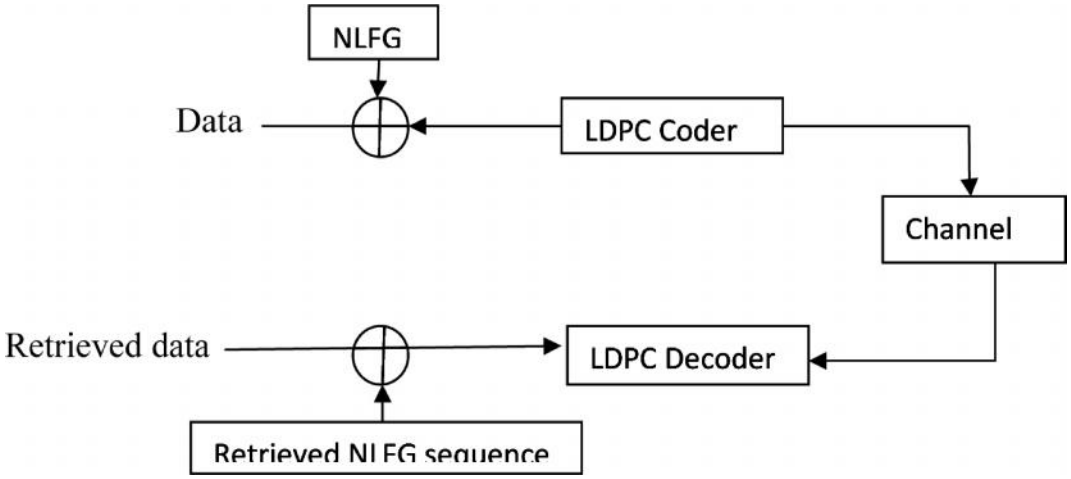
Proposed Method for Combining Channel Coding with Encryption

Earlier work for combining channel coding with cryptography makes use of LDPC codes for implementing McEliece cryptosystem, which is a public key cryptosystem (McEliece, 1978). Even though the security of these systems are pretty high, the complexity in implementation is too high and used by resource constrained devices. Hence we propose to use this channel coding method as a part of symmetric key cryptosystem in such a way as to increase security of a symmetric key cryptosystem.

The encryption can be done by ex-oring the data with output of Non Linear Filter Generator (NLFG) and channel coding can be done with LDPC coder. At the receiver side decoded data will be ex-ored with retrieved NLFG sequence. For a genuine receiver, the retrieved NLFG sequence is same as the actual keystream, since he knows the initial seed of the NLFG. An un-intended receiver tries to mount an attack on the NLFG and retrieves a sequence which is well correlated with actual keystream. The key used for generating key-stream of stream cipher is used for controlling the randomness in the construction LDPC codes. An unintended user will not possess the key and hence the coder structure will not be available for him. Hence the decoding and decryption will retrieve only very small portion of actual data without error. Thus an additional level of security can be introduced by controlling randomness in the LDPC encoding.

The performance of channel coder can be observed by comparing data and retrieved data in Figure 4 assuming initial key of NLFG

Figure 4: Block Diagram of Channel Coding and Encryption System



is known, while security of the system can be quantified by checking the correlation between the retrieved keystream and linear output of LFSR assuming initial key of NLFG and seed for construction of LDPC are not known.

Hence, we propose to introduce security in construction of H matrix of LDPC codes so that only an intended user can decode the channel code properly at the receiver. Hence the security of overall cryptosystem can be increased without any additional complexity in the system. Security can be introduced in the random or semi random construction methods of LDPC. The actual H matrix is not transmitted to the receiver on the open channel but only the seed used for construction of H matrix is transmitted. This also reduces transmission overhead. It is possible that this seed can be derived from actual key used in stream cipher, in which case the system doesn't demand any extra key bits.

Implementation of Security in Random Construction

In the Mackay random construction method the ones are introduced in various positions randomly as the first step in the construction of H matrix. These positions can be decided by the output of an LFSR, whose initial seed is a portion of key used for encryption. Then, an intended user who knows the key, can construct the actual H matrix. Hence there is no need to transmit the entire H matrix to receiver, which will help to reduce transmission overhead. For an un-intended receiver, since the key is not known H matrix is unknown. Hence the data cannot be decoded properly at receiver.

For example consider the construction of H matrix of size 255 x 510. Security can be embedded in its construction as explained below:

- Construct all zero matrix with size 255 x 510, i.e., $n = 510$, $= n - k = 255$.
- Consider ones per column $w_c = 3$, then ones per row $w_r = w_c\left(\frac{n}{m}\right)$. Then, the total number of one's required in H matrix = 510 x 3 = 1530.
- Choose the 8 bit LFSR as it produces 255 different states by giving the random seed.

- By giving six different 8 bit keys, one can get total 510 x 3 = 1530 different states within the range of 1 to 255.
- By using these states, ones are inserted in each column three times at different positions.
- Avoid length-4 cycles which degrade the performance of decoding algorithm.

SIMULATION RESULTS

Various experiments are conducted to evaluate the decoding performance of LDPC codes using random construction and semi-random construction. Also, the ability of secure LDPC codes to improve the overall security of a communication system without any additional hardware/computational complexity is well examined. Results of these experiments and the associated analysis are presented in detail here.

Comparison of BER Performance of Random LDPC Code Under Different Scenario

Figure 5 shows the BER plot of Mackay LDPC code under different scenario. The red curve indicate the bit error rate performance of Mackay (510,255) LDPC code for intended user, i.e., who knows H matrix structure. Green curve shows bit error rate performance of unintended user who doesn't know the structure of H matrix.

Six initial seeds of Linear Feedback Shift Register is taken as the key for getting H matrix, which is supposed to be known at the receiver. The code rate is 1/2 and the modulation scheme used is Binary Phase Shift Keying (BPSK). Channel model is AWGN (Additive White Gaussian Noise). 255 bits are transmitted in an experiment and the experiment is repeated 10000 times to get a point in the chart.

Figure 5: Comparison of (510,255,1/2) MacKay LDPC Code with Intended User and Unintended User, Girth = 6, dmin >=26

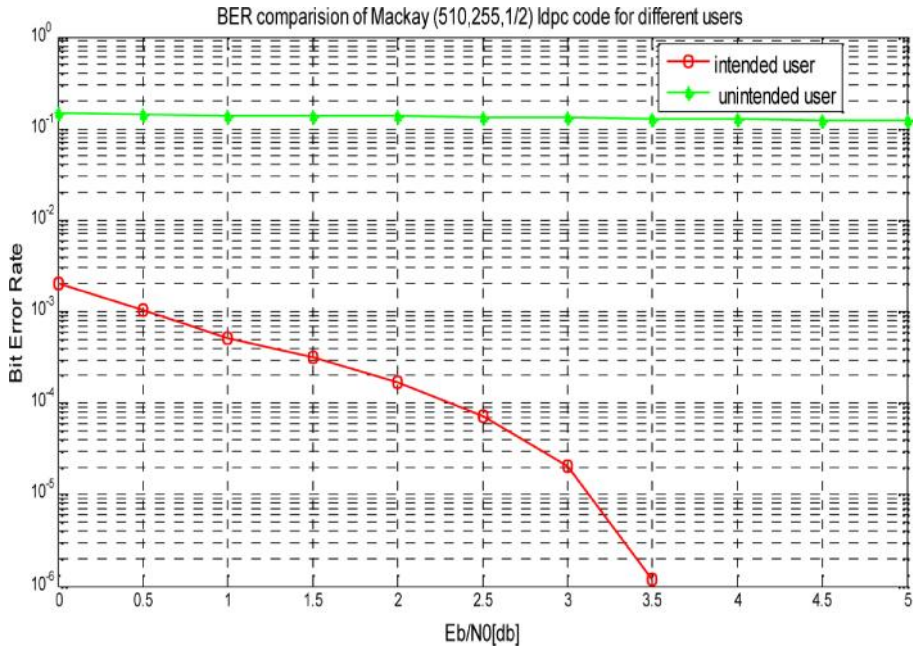
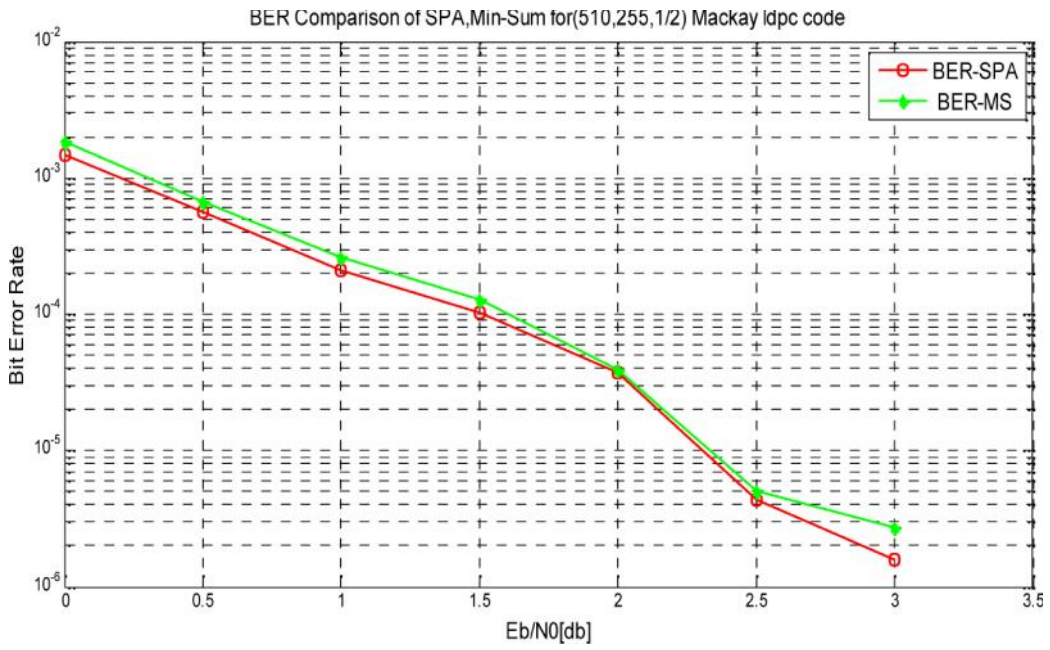


Figure 6: BER Comparison of (510,255,1/2) MacKay LDPC Code with Different Decoding Algorithms (1) Sum Product Algorithm, (2) Min Sum Algorithm



Comparison of BER Performance of Decoding Algorithms

Figure 6 shows the BER performance of random LDPC (510,255,1/2) code for two different decoding algorithms sum product and min sum algorithm, where min sum algorithm is approximation of sum product algorithm. The red curve shows the sum product algorithm in log domain and green curve shows the min sum algorithm.

CONCLUSION

Methods to improve the security of a communication system without any additional computational/hardware complexity is suggested in this paper. Error control coding is implemented using Low Density Parity Check codes efficiently for an intended user. But if secrecy is embedded in construction of H matrix, an un-intended user can get only a sub-optimal performance of the decoder. This makes it difficult to implement a known plain-text attack on the cryptosystem, since cipher text is not available in the correct form. This increases the computational complexity of cryptanalysis, thereby increasing security. So, when the devices are resource-limited, the proposed method provides a very good alternative to implement a very secure system without much computational complexity.

As a future work, more construction methods for LDPC can be tried as candidates to embed security. Then the best construction method can be identified in terms of minimum transmission overhead required.

REFERENCES

1. Baldi M, Cancellieri G, Chiaraluce F and De Amicic A (2009a), “Design of Multiple Serially Concatenated Multiple Parity-Check Codes for Wireless Applications”, in Proc. SoftCOM, Septeber, Split-Hvar-

Korcula, Croatia, Paper SS2-1569231445-2409.

2. Baldi M, Cancellieri G and Chiaraluce F (2009b), "New LDPC Codes Based on Serial Concatenation", 5th Advanced International Conference on Telecommunications.
3. Baldi M, Cancellieri G, Chiaraluce F and Carassai A (2009c), "LDPC Codes Based on Serially Concatenated Multiple Parity-Check Codes", *IEEE Communication Letters*, Vol. 13, No. 2, pp. 142-144.
4. Baldi M, Cancellieri G and Chiaraluce F (2009d), "A Class of Low Density Parity-Check Product Codes", 1st International Conference on Advanced in Satellite and Space Communications.
5. Bernhard M J Leiner (2005), "Low Density Parity Check Codes—A Brief Tutorial", Tutorial Paper.
6. Blahut R E (1983), *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, Inc., Reading, Mass.
7. Canteaut A (2005), "Fast Correlation Attacks Against Stream Ciphers and Related Open Problems", in Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW), October, Awaji Island, Japan.
8. Daniel J Castello Jr. (2009), "An Introduction to Low Density Parity Check Codes", Tutorial Paper.
9. Enricopaolini, GianluigiLiva and Marco Chiani (2003), "An Overview of Some Efficient Encoding and Decoding Algorithms for Low Density Parity Check Codes", in Softcom, 2003-10-10, Ancona, Italy.
10. Gallager R G (1962), "Low Density Parity Check Codes", *IRE Trans. Inf. Theory*, Vol. IT-8, pp. 21-28.
11. Jiang X and Lee M H (2009), "Semi-Random LDPC Codes with Efficient Encoding", *IEEE Electronic Letters*, Vol. 45, No. 24.
12. Jiang X, Yan Y and Ho Lee M (2010), "Semi-Random and Quasi-Cyclic LDPC Codes Based on Multiple Parity-Check Codes", IEEE ICC Proceedings.
13. Jonsson F and Johansson T (2001), "A Fast Correlation Attack on LILI-128", *Information Processing Letters*, Vol. 81, No. 3, pp. 127-132.
14. Lin S and Constello D Jr. (1982), *Error Control Coding: Fundamentals and Applications*, October, Prentice-Hall, Englewood Cliffs, NJ, USA.
15. Mackay D (1999), "Good Error-Correcting Codes Based on Very Sparse Matrices", *IEEE Trans. Inform. Theory*, Vol. 45, pp. 399-431.
16. Marco Baldi, Giovanni Cancellieri, Franco Chiaraluce and Amedeo De Amicic (2010), "Irregular M-SC-MPC Codes for Wireless Applications", European Wireless Conference, April.
17. Massey J (2001), "Step-by-Step Decoding of the Bose-Chaudhuri-Hocquenghem Codes", *IEEE Transactions on Information*.

18. Meier W and Staffelbach O (1988), "Fast Correlation Attack on Certain Stream Ciphers, Advances in Cryptography, EUROCRYPT88", *Lecture Notes in Computer Science*, Vol. 330, Springer-Verlag, pp. 301-314.

19. Menesis P, van Oorschot and Vanstone S (1996), *Handbook of Applied Cryptography*, CRC Press.

20. Michael Tanner R (1981), "A Recursive Approach to Low Complexity Codes", *IEEE Transactions on Information Theory*, Vol. IT-27, No. 5.

21. Tee J S K, Taylor D P and Martin P A (2003), "Multiple Serial and Parallel Concatenated Single Parity-Check Codes", *IEEE Trans. Commun.*, Vol. 51, No. 10, pp. 1666-1675.

22. William Ryan (2003), "Introduction and Overview of Low Density Parity Check Codes", Tutorial Paper.

23. Zongjie Tu and Shiyong Zhang (2007), "Overview of Low Density Parity Check Codes", Cit, 7th IEEE International Conference on Computer and Information Technology (CIT), pp. 469-474.

24. McEliece R J (1978), "A Public-Key Cryptosystem Based on Algebraic Coding Theory", DSN Progress Report, pp. 42-44.