Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/8981
DOI URL: http://dx.doi.org/10.21474/IJAR01/8981
ISSN NO. 2320-5407

RESEARCH ARTICLE

REVIEW ON USING BIOMETRIC SIGNALS IN RANDOM NUMBER GENERATORS.

Mohit Bansal, Hitesh Kardam, Himanshu Khairwal, Dr. Jyoti sharma and Ms. Sudha Narang.
Maharaja Agrasen Institute of Technology, Delhi, India.

Manuscript Info

Manuscript History
Received: 25 February 2019
Final Accepted: 27 March 2019
Published: April 2019

Key words:-
Random Numbers, Biometrics, Pseudo random numbers, randomness, Biometric Random Number Generators.

Abstract

Random numbers play an important role in digital security and are used in encryption, public key cryptography to ensure the safe and unchanged transmission. Random number generators are required to generate these random numbers, but true randomness is difficult to achieve and requires a true random source to generate the number which cannot be predicted from the knowledge of previous inputs. This paper discusses about incorporating biometrics and cryptography for stronger security and to generate random numbers with true randomness. Biometric systems are used to uniquely identify individuals in the security but uses a sophisticated procedure. Biometric signals are non-deterministic processes that are unpredictable and good source of randomness. This paper reviews the feasibility of using biometric signals in Random Number Generator (RNG) discuss whether biometric signals such as heartbeats, vascular patterns, iris scans and human Galvanic Skin Response (GSR) can be used in nearby future to generate reliable Random numbers. This paper will also review the work done towards generating random numbers using these biometric signals and the result of them, verified with statistical test suites such as NIST.

Introduction:-

True randomness is difficult to achieve and to generate Random numbers, Random Number Generators (RNGs) are used. To generate a random number, a true source of randomness is required which can be obtained through physical processes such thermal noise or through computation. Physical process offers better entropy source than computation-based entropy source, but are complex in nature, expensive to use and are hardware dependent. Generators. Thus, we need to rely on computational entropy source for RNGs to generate pseudo-random which are not truly random. Biometric signals are the non-deterministic physical processes that can be used to generate true random numbers in an efficient way and thus, biometrics can be used in cryptography.

1.1 Random Numbers

Random numbers are numbers with no pattern, that are unpredictable and non-reproducible from knowledge of previous inputs and are useful in lot of applications including cryptography and game theory. Random numbers are generated through Random Number Generators (RNGs) that uses an entropy source as the input which can be a physical source such as flipping a coin or thermal noise in electrons to generate a random number.

Corresponding Author:- Jyoti sharma.
Address**:** -Maharaja Agrasen institute of technology, Delhi, India.

Numbers generated through RNGs can be deterministic or non-deterministic based on the method used to generate them. Random Numbers have statistical properties with high entropy, which is the statistical measure of randomness. High Entropy means more randomness.

True Random Numbers are not easy to generate and there are certain properties for a number to be called random and the extent of the randomness defines the use case of the RNGs that generates the number. Thus, random number generation requires comprehensible knowledge of the generators used to generate Random Numbers. The entropy sources used to generate these random numbers needs to select intelligently and random sources for random numbers do not guarantee randomness in the numbers.

Properties of Random numbers:

1. Random and Pseudo random numbers generated for cryptographic applications should be unpredictable in nature, i.e. random numbers cannot be predicted based on the knowledge of previous outcomes.
2. To ensure unpredictability, care must be taken to decide on the entropy source used in the RNG and the seed used in PRNG.
3. The sequence should be generated from a Balanced binary Bernoulli source.

1.2 Random Number Generators

RNG (Random Number Generator) is a device used to generate a sequence of numbers that cannot be reasonably predicted better than by a random chance. Based on the entropy sources used to generate Random Numbers, they can be a True (Hardware) Random Number Generator (HRNG or TRNG) which generate genuinely random numbers or Pseudo Random Number Generator (PRNG) which generates numbers that look random but are actually deterministic in nature and can be reproduced if the state of the PRNG is known. True Randomness are difficult to generate and requires a comprehensible study of the entropy sources used to generate the random numbers.

As discussed above, source of entropy sources used to generate Random Number decides the nature of RNGs. When natural phenomenon and physical noises are used as the entropy source which are expected to be random in nature as they are incomprehensible to human minds, such as atmospheric noise, thermal noise of the electrons and other electromagnetic phenomenon, to generate random numbers. For example, cosmic background radiation or radioactive decay represent sources of natural entropy. The pattern of these natural phenomenon is difficult for one to predict and RNGs using such physical entropy sources are known as True Random Number Generator (TRNG). Random numbers generated by them follow the property of random numbers and one cannot predict them accurately. These RNGs though provide reliable source for random numbers, the speed at which entropy can be harvested from natural sources is dependent on the underlying physical phenomena being measured, making them slow and limits their use cases. They also require the comprehensible understanding of these complex physical phenomenon, are expensive in cost and hardware dependent i.e., the result of the RNG depends on the hardware used to generate or harvest the entropy source. That is, TRNGs are not an economical option to generate random numbers for tasks that is time critical.

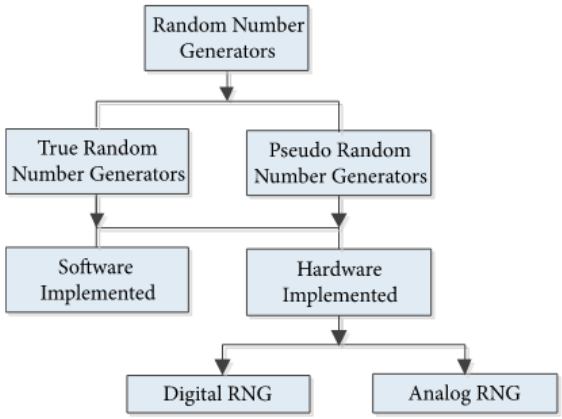
The other approach to generate Random Number that resembles true random numbers and are economical to generate uses computational algorithms that produce long sequences of apparently random results using an initial value known as “Seed” value. These RNGs are known are Pseudo Random Number Generator (PRNG) and are deterministic in nature, i.e., same seed value always generates same random number and the efficiency of these RNGs depends on the unpredictability of these Seeds and algorithm used to generate random numbers. These RNGs are not rate-limiting and can be used efficiently for time-critical processes. The algorithm used to generate Random number should not output same number for two different seed values and it should not be possible to determine the numbers based on the knowledge of previous numbers, i.e. the numbers generated should not have any pattern. Good statistical properties are central requirement for the number generated through PRNG. In general, careful mathematical analysis is required to have any confidence that a PRNG generates numbers that sufficiently close to random to suit the intended use. Various Techniques used in connection with random digits

This paper discusses about using physiological factors of human body as the entropy source to generate random numbers and the RNGs that uses these factors as the entropy source are known as Biometric Random Number Generator (BRNG).

Requirements for a Random number generator:

1. Random number Generators should not be blocking and compute random number in feasible amount of time.
2. The numbers generated should be unpredictable, and one should not be able to reasonably predict the next number in the sequence.
3. The entropy source used should behave as a balanced binary Bernoulli source of bits. Bernoulli source is a memoryless source whose output at time t is independent of what it produced before time t. Balanced means, that the a priori probability of all the outputs is equal.

Figure 1:-Random Number Generators



1.3 Biometric systems and RNGs

Biometrics have been used in cryptography for authentication purposes in security and to uniquely identify individuals. It refers to the identification and authentication methods that uses biometric signals to identify or validate a person's identity. Biometric signals can be categorized as Physiological and behavioral signals.[2] Biometric signals are physical processes and non-deterministic in nature that can be a good source of randomness for RNGs.

Physiological signals includes various traits of human body such as Finger prints, Galvanic Skin Response (GSR), Electrocardiogram (ECG) and Iris scan that is unique to every individual, developed in the early stages of embryonic development and most of the parameters remains constant throughout the life. Behavioral signals includes traits such as voice, signature and keystroke. The challenge in using these biometric system is the unreliability, the noise generated during the recording of these traits that affects their robustness to be used in authentication system. This paper discusses about using these biometrics signals as entropy sources in RNGs. These biometric signals are physical in nature and thus, BRNG is a type of TRNG. The efficiency of these biometric signals in RNGs will be reviewed along with the work done towards BRNGs so far.

Every human body is different and biometric signals are affected by various biological (internal) and atmospheric (external) factors, i.e., galvanic skin response changes with the temperature and body ionic concentration. Similarly, Heart rate can be recorded through ECG and EEG, and are random in nature. Previous recording of ECG cannot be used to predict the future reading as the ECG readings depends on the state of health of the heart that further depends on the lifestyle of the person.

So, how does these biometric signals used in identification systems that requires robustness in their pattern? Not all biometric signals fluctuates with the various physiological and atmospheric factors and signals that remains constant throughout our life are used in identification system, using the most reliable pattern in the signal that is most shielded to the noise during recording of them and makes use of the HDS (Helper Data Scheme). Concludingly, biometric signals are physical process that are random in nature and noise incorporated in recording and storage adds to the randomness. Also, various factors affects physiological processes and thus fluctuating biometric signals fluctuates are unpredictable making a promising source of randomness for RNGs.

1.4 Randomness and Entropy Measures

A random bit sequence is the result of any random, memoryless and unbiased physical process such as flipping of coin with sides labelled as "0" and "1". Each flip in this event, has probability of ½ and the outcome of next flip is independent of the previous flip. Randomness is the probability of the occurrence of an event and is measured through their entropy. To measure the randomness of a sequence to decide on its use case, various statistical tests are used to analyses them. Randomness is a probabilistic property, that is, the properties of a random sequence can be characterized and described in terms of probability. [3]

Why do we need to measure the randomness? Many RNGs in use are PRNG and the sequence generated by them are pseudo-random. To make sure that the sequence generated by these RNGs meets the required randomness for the task, statistical testing is performed on these RNGs.

NIST SP 800-22 test suite is widely accepted statistical testing package that consists of 15 different tests developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random or pseudo random number generators. These tests includes frequency test to check the proportion of zeroes and ones for the entire sequence, run test, longest run test and so on.

2. Literature Review

Various literature has been reviewed and discussed about the work done towards the approach of using biometric signals to be used for random number generation. Biometric signals are physical signals that can act as a good entropy source for RNGs and the random numbers generated are closely to truly random which is verified by testing their randomness on different statistical testing suites.

Different biometric signals can be used as the source and the result generated depends on the entropy or randomness measure of these signals as well as their method of recording them. Not all biometric signals can be used to generate Random Numbers and comprehensible tests needs to do before deciding on any signal to be used as the source and proper cryptanalysis is required.

Work towards BRNGs have been put forward by many researchers in the past, who verified feasibility of various biometric signals against statistical test suites such as NIST SP 800-22 are discussed in later sections.

2.1 Heart-Beat Rate

Heart beat rate is a biometric signal, that can be recorded easily using ECG or EEG and are useful in medical diagnosis of diseases. Heart-beat rate of an individual is a physiological phenomenon and the pattern of the ECG recorded depends on the health state of an individual. In the recent paper "Heart-Beats based biometric random binary sequence generation to secure wireless sensor networks" [4], a method is devised that uses ECG recording of 89 individuals were used to Generate Random Binary Sequence in order to secure the Wireless Body Sensor Networks (WBSNs) and suggests the Cryptography application of Heart-Beats. WBSNs are the wireless networks of wearable medical devices and wireless technologies that is being used for the medical purposes. Since wireless transmission of Health-related data contains confidential secrets in terms of privacy and thus requires the method to employ safe transmission.

The paper suggests a method to uses these heart beat rates to generate Random Binary Sequences (RBS) that is four times faster than the previous methodologies and the processing time required for the task is less than 8 seconds, which is suitable for real time health applications. 16 random bits are extracted from 8 concatenated Inter-Pulse Intervals (IPI) to generate 128-bit RBSs from an individual that can be used as keys for encryption required for secure transmission.

Hamming distance is used in this research to measure the uniqueness between IPI based binary sequences and to decide whether the generated RBSs can be used for the security purposes in WBSNs.

The pipeline followed in this research to generate the 128-bit RBSs are given as follows:

1. To detect the RR intervals from the ECG pattern, an efficient QRS detection algorithm having high detection rate of 99.3%.
2. The IPI sequences are generated in finite monotonic sequences, allowing the extraction of entropic bits from each IPI more efficiently.
3. A cyclic block encoding is used to convert IPIs into RBSs with least errors.

4. 16 random bits are extracted from each heartbeat and 8 such heartbeats are concatenated to produce 128-bit RBS.

The results were verified with NIST test suite and it is concluded that the method suggested is efficient in terms of processing and encoding time to generate Biometric RBS for WBSN based systems. The study also suggests the results degrade if more than 16-bits are extracted from each heart-beat. Similar application of ECG in Random Number generation is discussed in the paper, "ECG-RNG: A Random Number Generator based on ECG Signals and Suitable for Securing Wireless Sensor Networks" [6].

Table 1:-Result Comparisons of RBS generated from 3 groups of Heart beats (p-value) from work done in [4].

S. No.	Statistical test	Normal Healthy Subject (P – value)	MIT database Subjects (P-value)	Cardiac Patients (P-value)
1	F – Test	0.782	0.758	0.769
2	N – Test	0.993	0.990	0.986
3	B – Test	0.764	0.755	0.761
4	R – Test	0.862	0.721	0.698
5	Lr – Test	0.217	0.304	0.168
6	FFT – Test	0.038	0.026	0.031
7	Lc – Test	0.963	0.956	0.915
8	Ae – Test	0.997	0.995	0.992
9	C – Test	0.791	0.786	0.704

In the article, "Heartbeats do not make good pseudo random number generators: An analysis of the randomness of the Inter-Pulse Intervals" [5], the suspicion of using IPI as the source of randomness which is the basis of the method suggested in paper [4] is raised. According to the research done in paper [5], there were weaknesses in the previous study that considers Heart-beats a source of randomness. First, tests were only performed to test the entropy of generated random bit sequence are random or not. Furthermore, the datasets used in previous research are smaller in size, are not public and contains ECG from both healthy and diseased patients, that makes it unfit for the proper analysis. It also suggested that Least Significant bits of the IPI contain higher entropy.

After analyzing 19 public databases on ENT and NIST STS test suites, it is concluded that, short sequence of bits derived from an ECG record may seem random, but their use in cryptography applications remains questionable if large sequence is extracted, thus, large files from long ECG records should not be used.

2.2 Approach towards Vascular Patterns

Research on using vein patterns were done by Daniel Hartung and his colleagues, on using vascular patterns to generate True Random Numbers were published in the paper, "Towards a Biometric Random Number Generator – A General Approach for True Random Extraction from Biometric Samples." [7].

In the paper, Biometric systems and the noise associated with their storage were discussed along with the vein patterns that are developed during embryonic vasculogenesis that are influenced by random factors as suggested by the study done in paper [8]. The dataset of 10800 finger vein images were used in raw and various processed form (using morphological operators), from all 10 fingers of 45 subjects in 12 sessions. Each image of size (111 x 401) pixels, were used to estimate their entropy. The pipeline followed in the research is given as following:

1. Image is binarized in order to balance the number of ones and zeroes in the sequence in such a way that, the bit value of $I^{bin}(x,y)$ of every pixel I(x,y) at position (x,y) is computed "0" if I(x,y) is less than the interclass mean image of training set (I^{mean}), else, it is computed as "1".
2. Feature vector, F(x, y) is generated concatenating from image I's column which is later binarized in the same manner.
3. Each pixel position in F(x, y) is tested for its reliability and unreliable pixels were used in generating Random numbers.
4. A hash function is introduced to increase the entropy.
5. The result is tested against NIST test suite for Raw Images, Segmented Images and Skeleton Images of Finger vein patterns with and without hash function.

It is concluded that the images with more distinct features that is, Segmented and Skeleton images of finger vein patterns generated better results which is improved even further by introducing Hash functions.

Table 2:-NIST Experimental result, using different stages of vascular patterns in RNGs.

Source	K	Lambda	Length Bit Stream	Hash- Bit Stream	Result
I raw	25165	X	135000	100	5.6%
I raw	25165	157	135000	100	87.9%
I raw	25165	78	67000	100	93.4%
I opt	26930	X	145000	100	69.3%
I opt	26930	168	145000	100	98.2%
I opt	26930	84	72000	100	98.2%
I Seg	19211	X	100000	100	66.9%
I Seg	19211	120	100000	100	98.1%
I Seg	19211	60	50000	100	97.2%
I Skl	8003	X	43000	100	1.4%
I Skl	8003	50	43000	100	95.3%
I Skl	8003	25	21000	100	97.9%

Table 3:-Entropy Estimation of vascular image patterns in different forms.

Source	Entropy (bits)
Iraw	25165
Iopt	26930
Iseg	19211
Iskl	8003

2.3 Iris (and Retina) Scans

Patterns of Iris is unique for everyone and is developed in the embryonic stage in a non-deterministic fashion. Work towards iris based Random Number Generator is discussed in paper, "Biometric-Iris Random Key Generator Using Generalised Regression Neural Networks" [9], and "A novel iris and chaos based random number generator" [10]. In both papers, images of iris are used as biometric signals to generate RBS. The challenge discussed, common, in both papers is how to use the iris scan of same person at two different point of time to generate unique RBS. In [9], the imperfections or noise incorporated during the recording of Iris scan is suggested as the solution to this problem, while in [10], a chaotic function is introduced that extracts a unique edge pattern during the process of converting Iris scan into binary patterns.

In paper [9], the pipeline to generate Random Bit Sequence (RBS) is given as following:

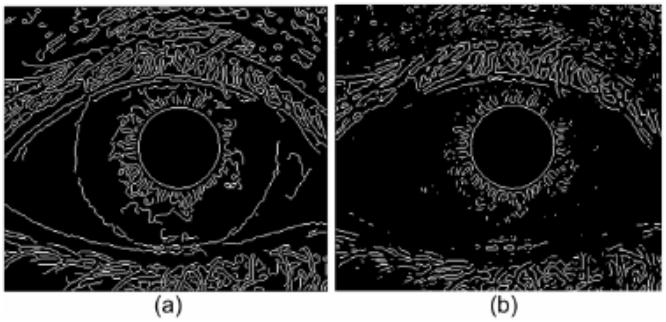
1. Iris is located using Integro-differential operators which outputs the rectangular area of Iris from the eye.
2. A set of Gabor filters are applied to extract useful characteristics from the Iris area.
3. These extracted features are then divided into groups to generate Random Bits in the next step.
4. These groups are then passed through Generalized Regression Neural Net (GRNN) Classifiers to generate bits for each group. GRNN is used due to its fast learning time and requires only one tuning parameter.

Paper [10] uses a different approach that uses a chaotic function that adds to the randomness in the Iris scans used. The results were tested on NIST SP 800-22 test suite. The technique followed in this paper is given as following:

1. Iris image is collected through database or human subject.
2. Relevant characteristics from the images are extracted through various edge detection techniques. To uniquely extract features from the same eyes, a chaotic function is introduced that process the Raw Iris images resulting in different Edges.
3. Edge detector generates a binary image of the edges from iris scans which when selected generates a random sequence, that is, next bit in the sequence cannot be predicted knowing the previous bits.

Both papers approached the same problem of generating a true random number, differently, but concluded that Iris patterns can be used as non-deterministic source for Random Number Generation, which passes all the randomness tests. Thus, Iris scans can be used as entropy source for RNGs.

Figure 2: Different edge detection from the iris scan of same source using Chaotic functions.



2.4 Galvanic Skin Response

Entire human skin is covered with sweat glands which excretes sweat to maintain the ionic balance and our body temperature. Galvanic skin response is a type of Electro-dermal Activity (EDA), that refers to changes in sweat gland activity. These changes in the sweat gland, are the reflection of our emotional and physical state (affected by external and internal factors). Sweat secretion also changes the skin conductance along with the thermo-regulation which can be used as entropy source to generate Random numbers.

In the work discussed in [11], a new approach, "Last fluctuating bit" is discussed on two types of biometric signals, "Human Galvanic response" and "Animal Neuro-physiological brain responses" and were examined as source of randomness.

The approach suggests that during the recording of any physical process, the least significant digits exhibit random properties. Thus, last fluctuating digit is used as random bit sequence over time when physical processes are digitized or binarized. Even though the recording of brain signals is complex and using galvanic Skin Response requires more processing time, their RNG passed NIST test suite as well as other test suites.

Conclusion:-

Biometric signals are physical processes that are non-deterministic in nature and can act as good source of randomness to generate True random numbers. In this paper, we reviewed the work done towards using Biometric signals in generating Random Numbers so far. Each biometric signal can be either physiological or behavioral process, each having their unique advantage as entropy source for a RNGs. All these biometric signals discussed here are non-deterministic and since, unlike finger prints, they cannot be left behind, one feel more confident using them as the entropy source.

Heart-Beats is one of the most promising biometric signals which can be used to generate Random numbers using IPI with few limitations. If more than a certain number of bits are extracted from a single ECG, the performance may degrade. Vascular patterns in fingers when used in processed skeleton form along with hash function, generates a good result and can be used in various cryptography applications. Iris scans can be challenging to use as Iris patterns remain constant throughout the life, but operations can be used to generate unique pattern from the same images and can act as a reliable Entropy source. Galvanic Human Response do not have fast sampling rate when used with last fluctuating digit method.

Biometrics are used in cryptography to generate Random numbers along with the authentication and identification of individuals. Future work towards biometric random number generators will be improved with better medical equipment to record sophisticated medical data easily and improved feature extraction algorithms.

References:-

1. J. Von Neumann, "Various techniques used in connection with random digits," Applied Math Series, Notes by G. E. Forsythe, in National Bureau of Standards, Vol. 12, pp. 36-38, 1951.
2. Eng, A.; Wahsheh, L.A. Look into my Eyes: A survey of Biometric Security. In Proceedings of the 2013 Tenth International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, USA, 15-17 April 2013: pp. 422-427.
3. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker. "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc Mclean Va, vol. 1, no. 1, pp.1-164, 2001.
4. Pirbhulal, Sandeep & Zhang, Heye & Wu, Wanqing & Mukhopadhyay, S.C. & Zhang, Yuan-Ting. (2018). Heart-Beats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks. IEEE Transactions on Biomedical Engineering. PP. 1-1. 10.1109/TBME.2018.2815155.
5. Ortiz Martin, Lara & Picazo-Sanchez, Pablo & Peris-Lopez, Pedro & Tapiador, Juan. (2018). Heartbeats Do Not Make Good Pseudo-Random Number Generators: An Analysis of the Randomness of Inter-Pulse Intervals. Entropy. 20. 94. 10.3390/e20020094.
6. Camara C, Peris-Lopez P, Martín H, Aldalaien M. ECG-RNG: A Random Number Generator Based on ECG Signals and Suitable for Securing Wireless Sensor Networks. *Sensors (Basel)*. 2018;18(9):2747. Published 2018 Aug 21. doi:10.3390/s18092747
7. Hartung, Daniel & Knut, Wold & Graffi, Kalman & Petrovic, Slobodan. (2011). Towards a Biometric RandomNumber Generator - A General Approach For True Random Extraction FromBiometric Samples.. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI). 267-274.
8. Eichmann, Anne & Yuan, Li & Moyon, Delphine & Lenoble, Ferdinand & Pardanaud, Luc & Breant, Christiane. (2005). Vascular development: From precursor cells to branched arterial and venous networks. The International journal of developmental biology. 49. 259-67. 10.1387/ijdb.041941ae.
9. Garza Castañón L.E., Pérez Reigosa M., Nolazco-Flores J.A. (2006) Biometric-Iris Random Key Generator Using Generalized Regression Neural Networks. In: Ali M., Dapoigny R. (eds) Advances in Applied Artificial Intelligence. IEA/AIE 2006. Lecture Notes in Computer Science, vol 4031. Springer, Berlin, Heidelberg
10. Zhu, Hegui & Zhao, Cheng & Zhang, Xiangde & Yang, Lianping. (2013). A novel iris and chaos-based random number generator. Computers & Security. 36. 40–48. 10.1016/j.cose.2013.02.003.
11. Szczepanski, Janusz & Wajnryb, Eligiusz & Amigó, José & Sanchez-Vives, Maria & Slater, Mel. (2004). Biometric random number generators. Computers & Security. 23. 77-84. 10.1016/S0167-4048(04)00064-1.