SECURE KEY TRANSFER PROTOCOL USING GOLDBACH SEQUENCES

By

KRISHNAMA RAJU KANCHU

Bachelor of Technology in Computer Science

Sir M. Visvesvarayya Institue of Technology

Bangalore, Karnataka, India

2011

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
May, 2013

SECURE KEY TRANSFER PROTOCOL USING

GOLDBACH SEQUENCES

Thesis Approved:

Dr. Subhash Kak

Thesis Adviser

Dr. Nophill Park

Dr. David Cline

Name: KRISHNAMA RAJU KANCHU

Date of Degree: MAY, 2013

Title of Study: SECURE KEY TRANSFER PROTOCOL USING GOLDBACH SEQUENCES

Major Field: COMPUTER SCIENCE

Abstract: This thesis presents a method of communicating keys using sequences obtained from the partitions of even numbers as primes, which is the Goldbach conjecture. We have investigated the randomness properties of these sequences. New variants of the prime partitions are examined and it is found that the sequences so obtained also have excellent cross correlation properties. An algorithm is devised where the Goldbach partitions are used to exchange keys via a certification authority.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER I

INTRODUCTION

Protocols for security

Different techniques and protocols are used for security applications. Some of these are based on number theory [1]-[7], whereas others are based on physics [8]-[12]. Some applications use hashing algorithms such as SHA-1, SHA-2, GOSH, HAVAL, MD-5. For key distribution symmetric and asymmetric methods are used. Amongst the protocols and hierarchies proposed for secure communication are: Internet Key Service layered on Secure DNS, Session key distribution in three party setting of Needham and Schroeder, Password-based protocols for authenticated key exchange against a dictionary attack and methods for reliable multicast [1].

Cryptography has been most successfully deployed in protocols where a client-server relationship exists, such as Secure Socket Layer (SSL) and Transport Layer security(TSL). A data can be encrypted using an encryption algorithm along with a public key. This encrypted data could be read by the node which has the private key of this encrypted data which can decrypt the message. A signature is formed together with a message digest and a private key. It makes it impossible to detect the message digest given a key and also it would be impossible to detect the key given a message digest. Other variations are given in [13],-[14].

In this thesis we consider a new way to develop a key distribution protocol using the standard Goldbach conjecture and its constrained forms. According to this conjecture any even number can be represented as a sum of two prime numbers. We have looked at random sequences obtained from the count of partitions of different even numbers and we have derived new variant sequences of this partition random sequence. Random sequences can be good candidates for cryptographic keys [15]-[18] and they have other applications in cryptography. When random sequences from different sources are used, their independence may be checked by a cross correlation analysis [19]-[21].

Goldbach partitions will be shown to have excellent cross correlation properties. We also present the use of Goldbach partitions for a key exchange protocol.

.

CHAPTER II

REVIEW OF LITERATURE

Goldbach sequences

In 1742, Goldbach stated that every even number can be represented as the sum of three prime numbers, at that time he considered one as a prime number. Later, Euler restated Goldbach hypothesis as any even number greater than four can be represented as a sum of two prime numbers [22],[23]. This is also called as strong conjecture. And the numbers of such prime pairs are called as partitions. Examples are:

6 = 3+3	(one partition)
8 = 3+5	(one partition)
10 = (3+7) or (5+5)	(two partitions)
12= (5+7)	(one partition)

Below is the count for partitions for n up to 36 where g(n) is the partition count. This table shows how the partitions grow randomly as the numbers increase.

Table1. Number of partitions of g(n) for an even number n

N	20	22	24	26	28	30	32	34	36
g(n)	2	3	3	3	2	3	2	4	4

Several number theoretic techniques are used for the generation of random numbers. We wish to introduce another method that generates pseudo-random numbers using Goldbach partitions. Note, further, to prove the falsity of the Goldbach conjecture it requires that for n, all instances of $n-p_i$ for consecutive odd primes p_i up to n/2 be non-prime. But, prime number theorem says that the probability of a selected number m being prime is given by 1/ ln m therefore, the probability of not being prime is (1- 1/ln m) and hence the conjecture being false is $\pi(1- 1/p_i)$ which decreases as n increases.

Goldbach series are the those number sequences which are generated as a result of Goldbach conjecture that all even numbers greater than two can be expressed as a sum of two prime numbers. Figure 1 presents the partitions for numbers less than 1,000,000.

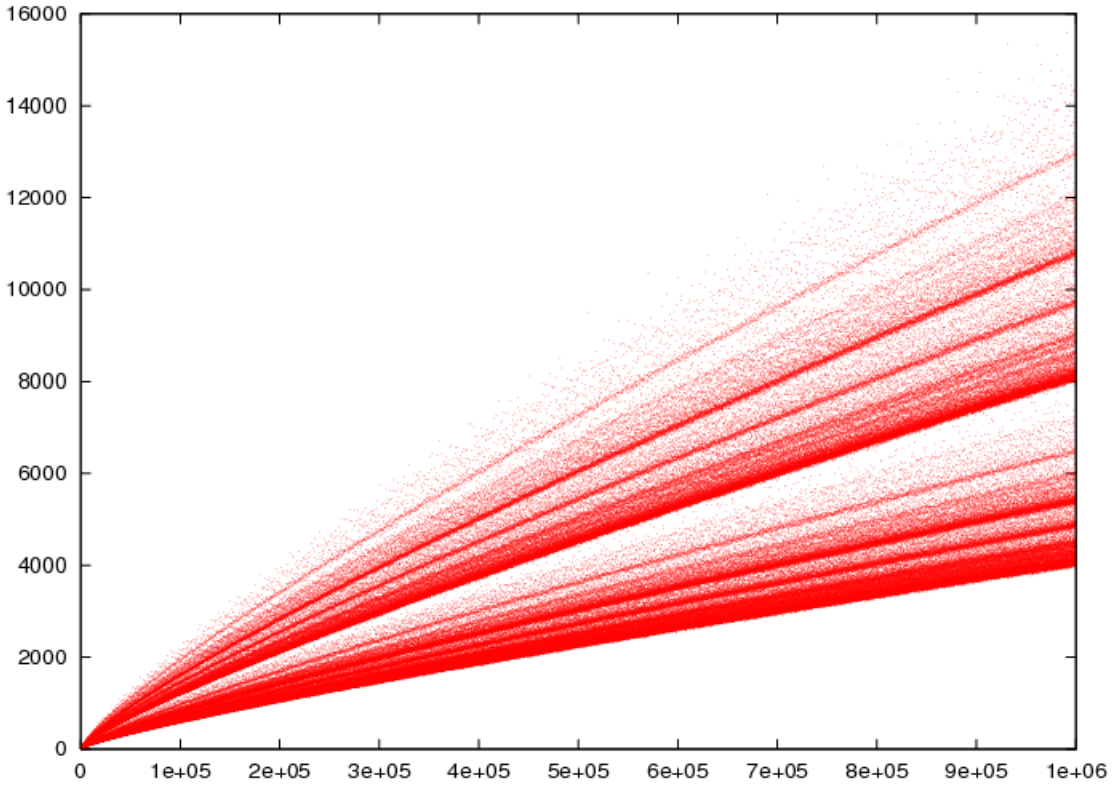

Figure 1. Goldbach partitions for the even number less than 1,000,000 (Source *Wikipedia Commons*).

The points may be grouped into several regions as observed from the bold regions in the above graph. It is also likely that even numbers with distinct partitions could be found as the value of the number increases. It is also observed that there are peak values as the numbers increase. These peak values occur for numbers that are product of several small prime numbers.

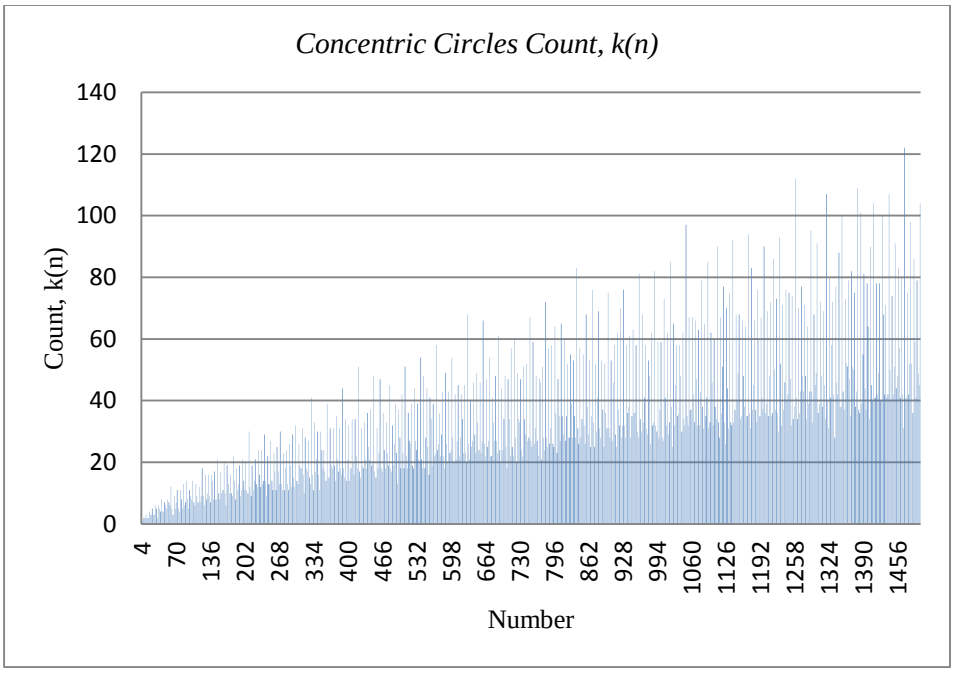

Figure 2. Graph showing distinct peaks for numbers that are integral multiples of prime.

The peaks start from 15, 30, 60 , 90, 210,.. and they range up to largest product of prime numbers within our set.

CHAPTER III

METHODOLOGY

Goldbach Partitions and their Behavior

Goldbach partitions represent the number of ways an even number can be represented as a sum of two prime numbers. The Goldbach partitions when observed on close quarters would produce some interesting behaviors. One of those, which enable the use of Goldbach partitions in cryptography, is the local peaks values and autocorrelation property.

In order to study the local peak values we need to understand the partition count for each even number. The partition count of all even numbers consists of series of independent values of even and odd numbers whose occurrences can be ascertained through the autocorrelation properties which describe the correlation between the variable across different ranges of separation.

When a graph of partitions versus count is plotted, it is seen as below.

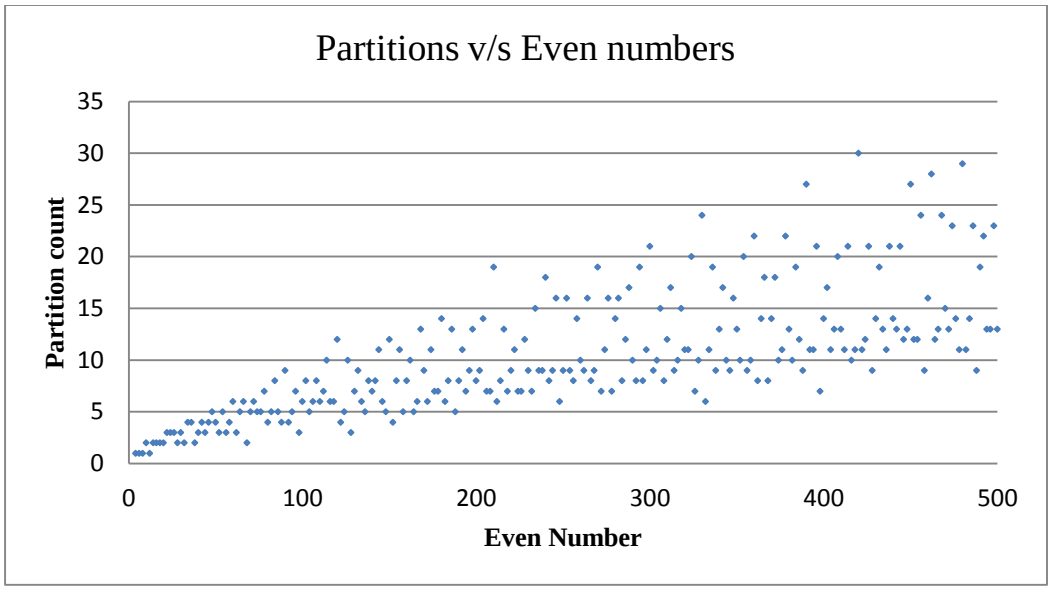

Figure3. Graph representing partitions for even numbers

The partition count of the even numbers till 188 is shown in the table below,

Table2. Partition count for numbers less than 190

n	g(n)	n	g(n)	n	g(n)
4	1	66	6	128	3
6	1	68	2	130	7
8	1	70	5	132	9
10	2	72	6	134	6
12	1	74	5	136	5
14	2	76	5	138	8
16	2	78	7	140	7
18	2	80	4	142	8
20	2	82	5	144	11
22	3	84	8	146	6
24	3	86	5	148	5
26	3	88	4	150	12

28	2	90	9	152	4
30	3	92	4	154	8
32	2	94	5	156	11
34	4	96	7	158	5
36	4	98	3	160	8
38	2	100	6	162	10
40	3	102	8	164	5
42	4	104	5	166	6
44	3	106	6	168	13
46	4	108	8	170	9
48	5	110	6	172	6
50	4	112	7	174	11
52	3	114	10	176	7
54	5	116	6	178	7
56	3	118	6	180	14
58	4	120	12	182	6
60	6	122	4	184	8
62	3	124	5	186	13
64	5	126	10	188	5

When a graph is plotted for this count up to a sequence of 2000 numbers we would get a graph as follows

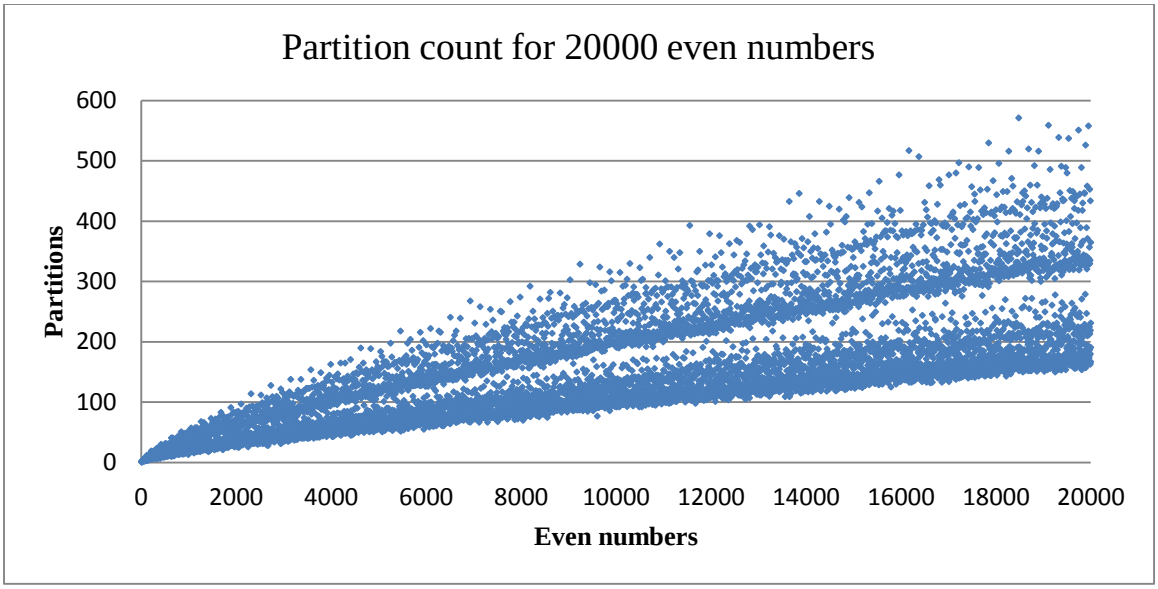

Figure4. Pattern representing the partition count for 20000 even numbers

We see a set of local peaks existing for each number as the range increases. The peaks occur for the numbers which are multiple prime and a product of the prime numbers and its multiples.

We observe peaks for 2×3 = 6; 2×3×5 = 30; 2×3×5×7= 210; 2×3×5×11=330; 2×3×5×13=390; 2×3×5×7×11=2310; 2×3×5×7×11×13=30030; 2×3×5×7×11×13×17=510510; 2×3×5×7×11×13×17×19=9699690…

Table3. Peak values for prime numbers' product and its adjacent numbers

n	g(n)	n	g(n)	n	g(n)	n	g(n)
30020	318	60050	524	90080	741	1021010	5567
30022	240	60052	397	90082	577	1021012	4163
30024	470	60054	798	90084	1119	1021014	8402
30026	223	60056	406	90086	578	1021016	4518

30028	237	60058	410	90088	552	1021018	4127
30030	905	60060	1564	90090	2135	1021020	17075
30032	225	60062	387	90092	552	1021022	4401
30034	224	60064	394	90094	547	1021024	4140
30036	466	60066	846	90096	1110	1021026	8228
30038	232	60068	400	90098	594	1021028	4179

This above table represents the partition value of the number which is a product of the prime numbers and partition values of its adjoining numbers. It is clear that the peak values are two to three folds greater than its adjacent numbers. This observation may be mathematically represented as follows

$g(6k) > g(6k+2)$

$g(30k) > g(30k+2)$

$g(210k) > g(210k+2)$

and so on…

Now we consider the autocorrelation property of the binary map of the sequence of partitions. The autocorrelation function is mathematically given by

$$C(i) = \frac{1}{n} \sum \quad a_m \, a_{m+i}$$

In order to study the autocorrelation properties, we take first 2000 even numbers starting from 4 and count the number of partitions for each even number. We divide the partitions into two groups which are the 0 group and the 1 group. Numbers which have an even partition count are represented as 0 and numbers which have an odd partition count as 1. Hence, the table would be as follows.

Table4. Representation for binary (0,1) mapping of partitions of even number n

n	20	22	24	26	28	30	32	34	36
g(n)	0	1	1	1	0	1	0	0	0

This set of sequences is thus converted to a sequence containing -1 and 1 where 0 represents -1 and 1 represent itself. This is represented in Table 3.

Table5. Representation for binary (1,-1) mapping partitions of even number n

n	20	22	24	26	28	30	32	34	36
g(n)	-1	1	1	1	-1	1	-1	-1	-1

The autocorrelation sequence thus obtained when plotted on a graph is shown in Figure 5. The peak value |C(k)| for non-zero k is 0.0745 which is quite low and which attests to the excellent randomness property of the Goldbach partition sequence. These sequences can thus be used in cryptographic applications.

In a variant of the above scheme each even number may be represented as a difference of two numbers. On determination of the number of partitions and the autocorrelation

function, we see that the autocorrelation function is a mirror image of the graph for which even number is considered as a sum of prime numbers.

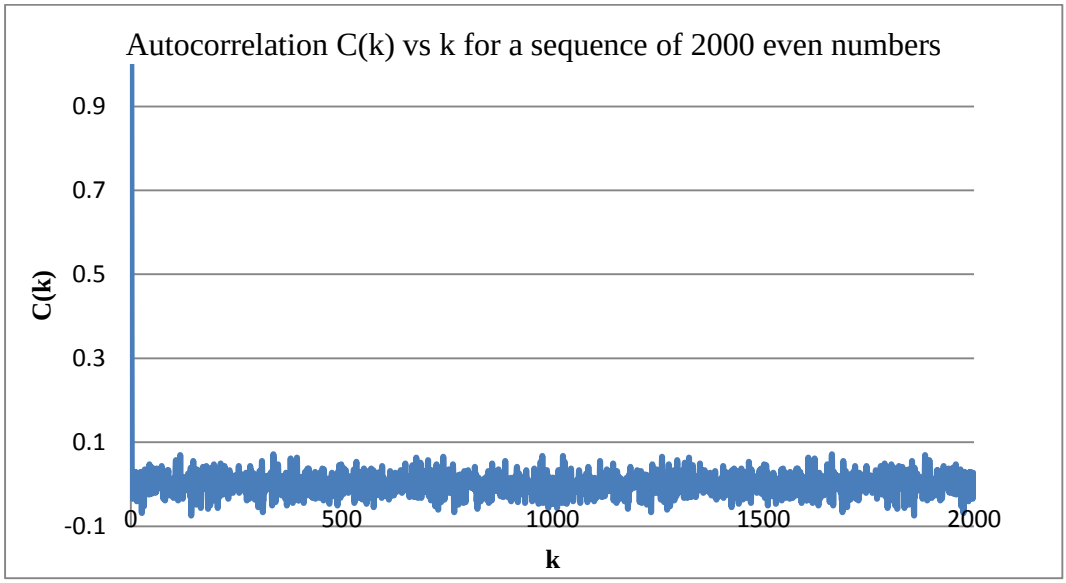

Figure5. Autocorrelation graph for a sequence of 2000 even numbers

Goldbach Circles and Goldbach Ellipses

We now consider partitions which are equidistant to the given number from both sides of a number. That is, an even number is represented as 2n and among all the possible partition; we select the partition which is nearest to n and equidistant from both sides of n. As example if we consider 28, then we have two partitions for it (5, 23) and (11, 17). We see that latter partition is closest and equidistant to 14. Hence we say its Goldbach radius as 3. A Goldbach circle with equal valued axes is termed a Goldbach circle.

We can generalize the notion of Goldbach circle to an ellipse where the axes are of different values. We consider an ellipse (l, k) for an even number n such that n and k are co-primes. That is n is a multiple of either 1 or k. Here is the number line representation of the ellipse for a k value equal to 5

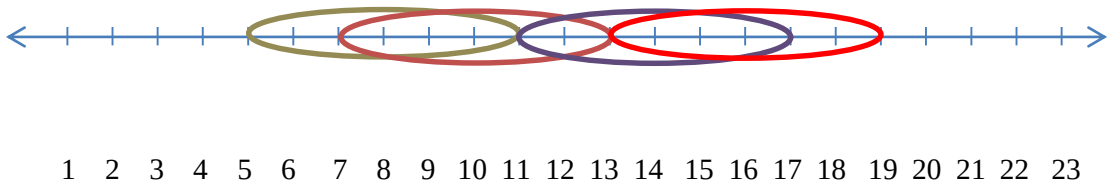

Figure 6. The Goldbach ellipse of numbers 6, 8, 12 and 14 for k=5

One of the characteristic numbers in the Goldbach ellipse is 4n + (k-1)m. Hence, when 2n is mapped on 4n+(k-1)m we see a cryptographic application in the form of determining m sequence. For different values of k we get different m sequences. We show how the m sequence varies for different k sequences in the following table.

Table 6. Ellipse characteristic values for k =7

2n	2n-m	2n+km	M	4n+(k-1)m
4	3	11	1	14
6	5	13	1	18
8	5	29	3	34
10	7	31	3	38
12	11	19	1	30
16	13	37	3	50
18	13	53	5	66
20	17	41	3	58
22	19	43	3	62
24	23	31	1	54
26	23	47	3	70
30	29	37	1	66
32	29	53	3	82
34	19	139	15	158

Similarly, a table for k = 3 may be drawn.

Table7. Ellipse sequence for k = 3

2n	2n-m	2n+km	m	4n+(k-1)m
4	3	7	1	10
8	7	11	1	18
10	7	19	3	26
14	13	17	1	30
16	11	31	5	42
20	19	23	1	42
22	19	31	3	50
26	19	47	7	66
30	19	43	3	62
32	29	41	3	70
34	31	43	3	74

In both the tables we observe that there is no presence of integral multiples of k in the 2n column. This is because there can't be any ellipse generated for these numbers.

The cryptographic application of these ellipses can be found by analyzing the m sequences generated for each sequence with different k values. Let us consider the sequence where k = 7 in Table 6. In this case we have an m sequence with values like 1, 3, 5, 15… we can categorize these values into two groups by performing a mod 4 operation. Thus we get only numbers with 1 and 3 as shown below

Table8. m sequence which is categorized into 2 groups with k value =7

2n	4	6	8	10	12	16	18	20	22
m mod 4	1	1	3	3	1	3	1	3	3

Hence we can represent all 1 with 1 and all 3 with -1 and perform an autocorrelation function which gives the probability of predicting the numbers. The result is shown in Figure 7.

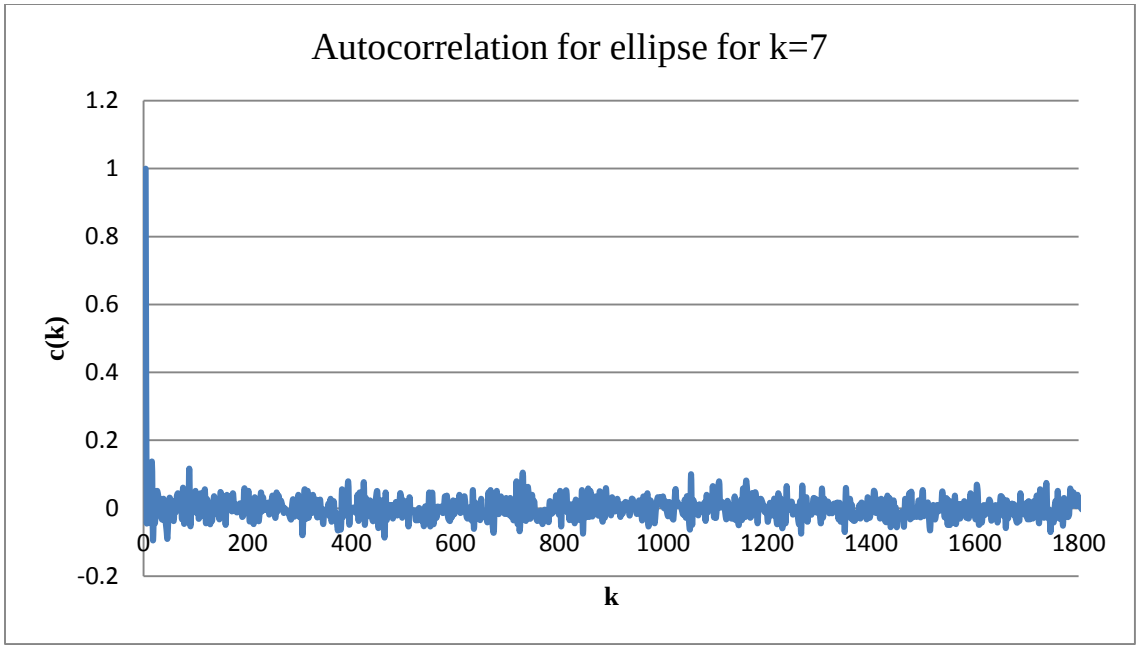

Figure 7. Autocorrelation function for an ellipse sequences with k = 7

The maximum probability of predicting the sequence is found to be 11% and it is observed that the probability of predicting the sequence decreases as the value of k increases because of more possible numbers and more data set and its associated ranges.

Goldbach Concentric circles

Unlike Goldbach circles, Goldbach concentric circles differ in its definition. In, Goldbach circles, we define the radius as the shortest equidistant partition from both the sides of the number. In this concentric circles, we define the possible number of Goldbach circles that are possible for a given even number.

The Goldbach circles for the first few even numbers are as shown below

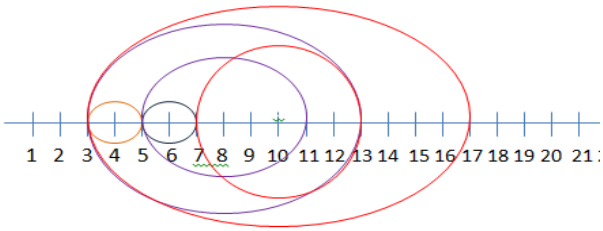

Figure8. Number line showing Goldbach concentric circles

Hence, we have a maximum bound on the number of such Goldbach concentric circles for each even number. The number of Goldbach circles is less than or equal to the number of prime numbers less than that number. We represent this sequence with the function k(n) of Table 9.

Table 9. Number of concentric circles k (n), n from 4 to 36

n	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
k(n)	1	1	2	2	3	2	2	4	3	3	5	3	3	6	5	2	6
k(n) mod *2*	1	1	0	0	1	0	0	0	1	1	1	1	1	0	1	0	0

As the even numbers in consideration increases the concentric circles count also increases with it progressively. The graphical analysis of this count gives interesting results.

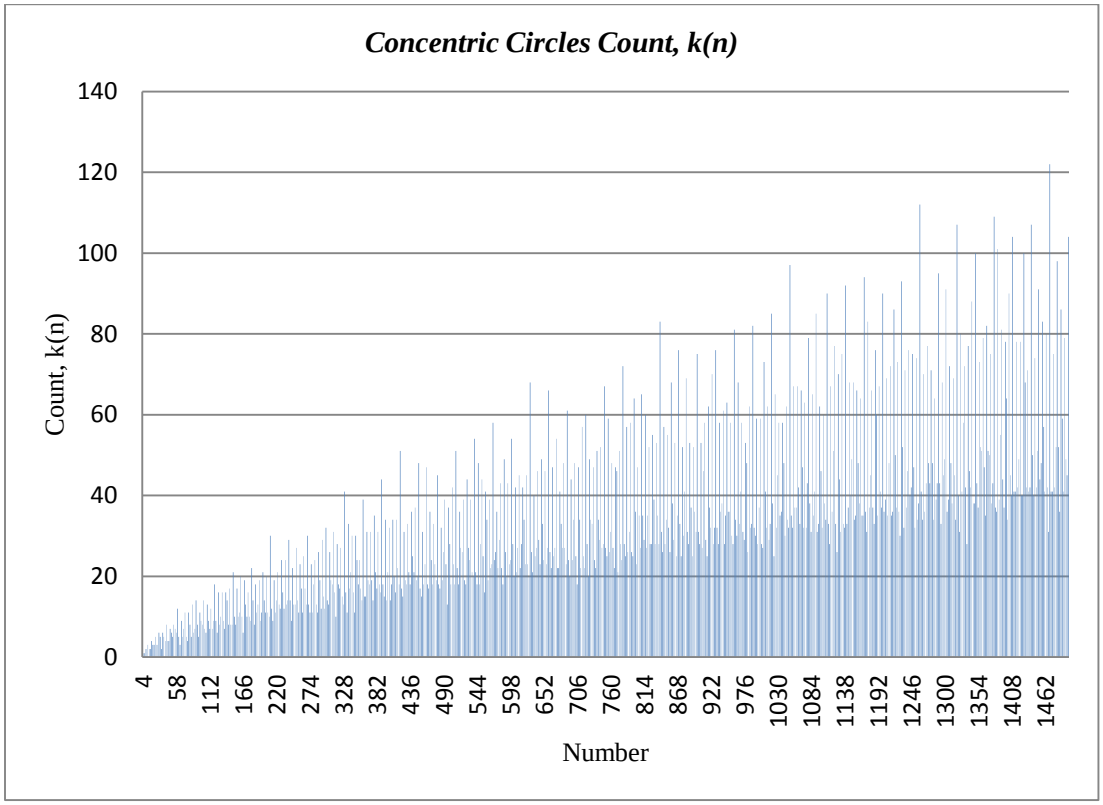

Figure 9. Concentric Circles graph against an even number for a count of 1500 numbers

On close observation we see the presence of peaks which are repeating at regular intervals. A few other local peaks repeat at equal intervals. This property is similar to the peaks for a Goldbach partition count. The peak value is at its peak for the numbers which are multiple of prime numbers and their integral multiples:

2×3 = 6; ; 2×3×5 = 30; 2×3×5×7= 210; 2×3×5×11=330; 2×3×5×13=390; 2×3×5×7×11=2310; 2×3×5×7×11×13=30030; 2×3×5×7×11×13×17=510510; 2×3×5×7×11×13×17×19=9699690, etc.

We also find that the values of these numbers are greater than its adjacent numbers. And also these values are three to four folds greater than its adjacent numbers:

$k(6n) > k(6n+2)$

$k(30n) > k(30n+2)$

$k(210n) > k(210n+2)$ and so on…

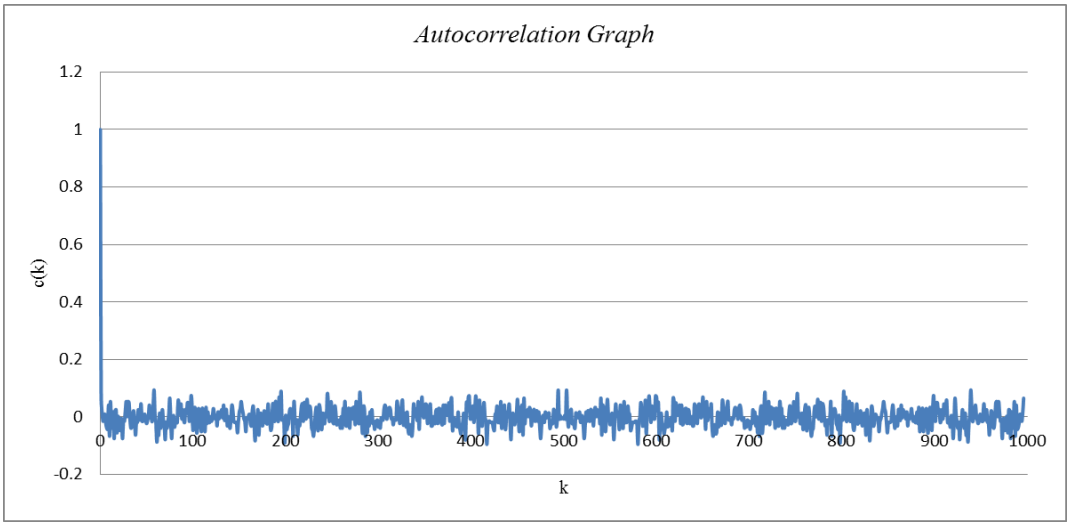

Figure10. Autocorrelation of the Binary Goldbach concentric count sequence.

Cross Correlation between various sequences

We now present results on the cross correlation of these sequences. The cross correlation of two sequences represents the interdependence of the two strings. The closer the values of it to zero, the lesser is the dependence.

If sequences are represented by a and b, then for a period of n the cross correlation between the two is given by the formula $C(k) = 1/n \sum_{k=0}^{n-1} b_i * a_{i+k}$.

The strings represented here are converted from their original values to 1, -1 representation as described above.

Here we present the cross correlation for the following sequences: Ellipse sequence on circle sequence; Ellipse sequence on ellipse sequence (with different k values); Goldbach concentric circle sequences on Goldbach circles.

1. **Ellipse Sequence on Circle Sequence**

We consider the Goldbach Ellipse sequence with k =7 and a Goldbach circle sequence. We consider the length of the test string to be 1700. Converting the test strings in a binary 1, -1 format we compute the cross correlation function as shown in Figure 11.

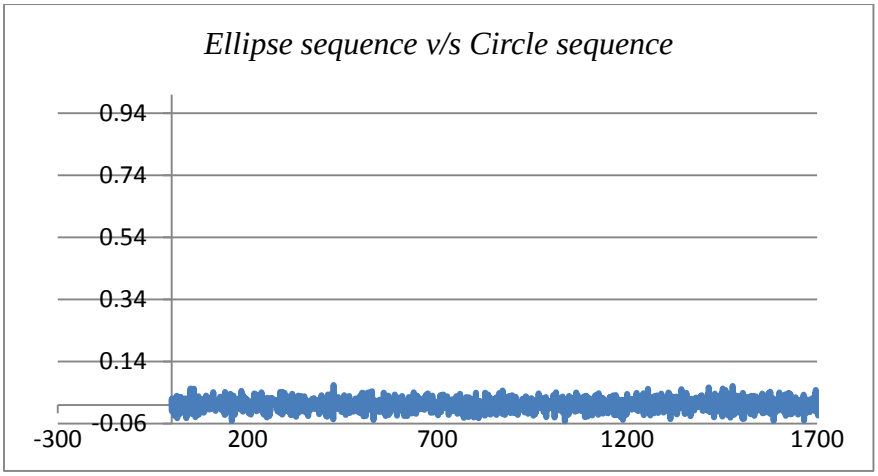

Figure11. Cross correlation between Goldbach Ellipse and Goldbach Circle.

The maximum cross correlation value, $|\max C_{(b,a)}|$ is found to be 7%. As shown in Table 10, the peak varies with the length of the sequence, which is to be expected.

Table10. Table showing the variation of peak $C_{(b,a)}$ for different length(n) strings.

n	*Range*
10	0.4
50	0.411
100	0.3267
250	0.1784
500	0.1497
750	0.1318
1000	0.1248
1250	0.0983
1500	0.1045
1750	0.0725
2000	0.0764
2500	0.0715
3000	0.0583
3500	0.0591
4000	0.0605
4500	0.0567
5000	0.0486

The peak value decreases as the length of the test string increases.

2. Ellipse sequence on Ellipse Sequence (With different k values)

Now we present the cross correlation between two ellipse with different k values of 5 and 7. The cross correlation is as shown below.

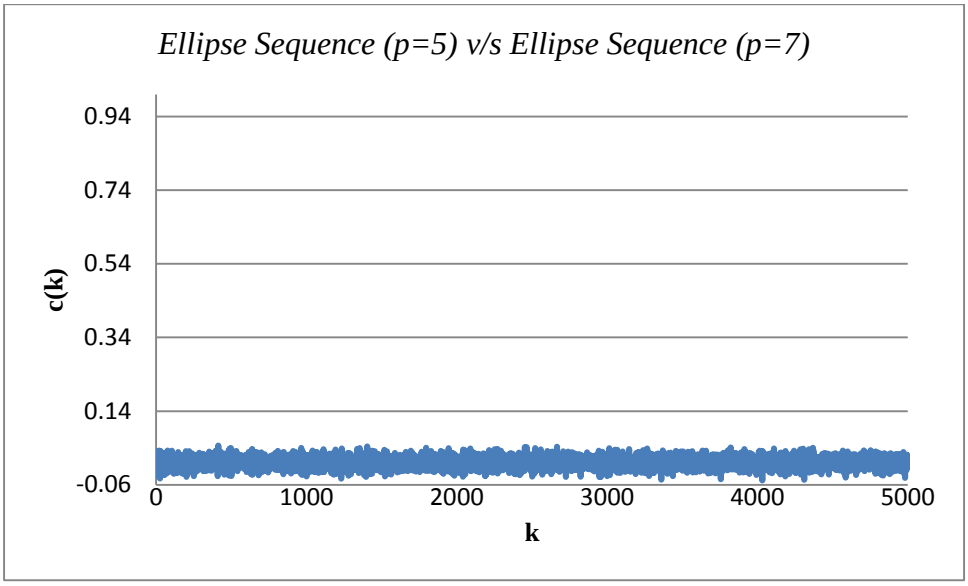

Figure12. Cross correlation between Ellipse k=5 and k=7. For 5000 numbers

Here the peak cross correlation value is 3%.

3. Goldbach Concentric circle sequences on Goldbach circles.

Next we consider the relationship between the Goldbach concentric circle in relation with Goldbach circles. The resulting cross correlation graph is as shown in Figure 13. Its peak value is less than around 4% for a sequence of length 5000.

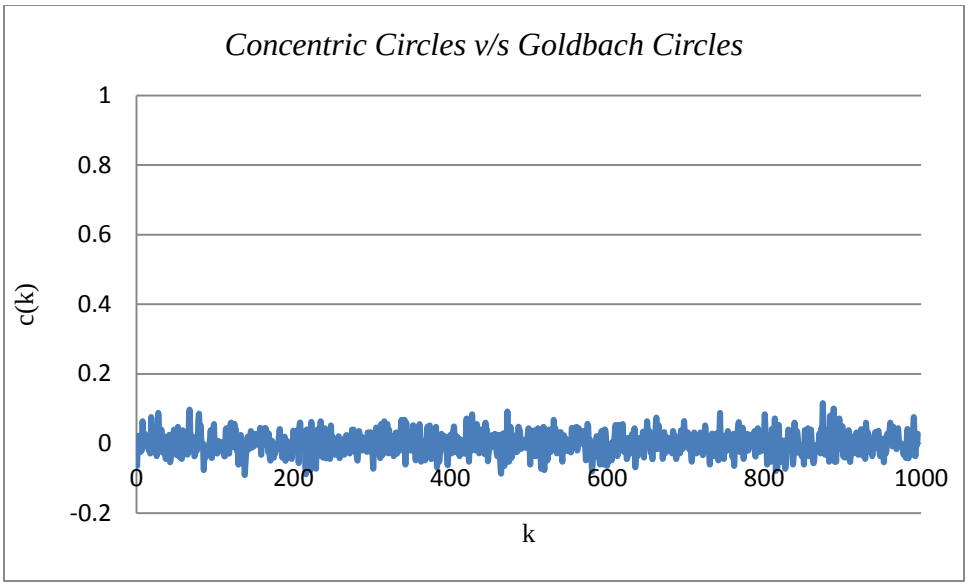

Figure13. Cross correlation between Concentric Circles and Goldbach Circles.

CHAPTER IV

COMMUNICATION PROTOCOL

We now present a secure communication protocol. Consider two peers that wish to communicate with each other in the presence of a Certification Authority who helps in authenticating the communicating parties with each other. The Certification Authority also enables to transfer the session key between the communicating parties.

It is assumed that secret keys of communicating parties A and B is a, b respectively. CA computes n= a + b which is used in the communication stage.

Protocol

When either of the communication party wishes to start a communication with its peer, a message is sent to the Certification Authority (CA) to set up the communication. At this stage, peer A sends a request message along with value k to the CA as shown below.

Peer A sends: $k \oplus h(a)$

Where h(.) represents a hashing function and $\oplus$ represents a modulus 2 addition of the numbers in the binary form. CA can determine the value k since it has the secret key of A which is a. Hence, the key k is determined by CA which is used to generate the binary

sequence by C.A. Thus, a Goldbach ellipse sequence, Goldbach concentric circles sequence or a Goldbach radius sequence is used to generate the binary sequence by C.A.

The sum n, which is generated by the sum of the two secret keys A and B is added with a random number to generate a new even number. The number of Goldbach partitions for this even number is determined and one of those Goldbach partitions are used as an index for selecting the binary sequence from the newly generated binary sequence which is generated by the Goldbach ellipse sequence. This binary sequence thus selected is sent to both the peers which are to communicate with each other with the help of their secret keys as follows,

Peer A receives: key $\oplus$ h(a)

Peer B receives: key $\oplus$ h(b)

where h(.) represents a hashing function and $\oplus$ represents a modulus 2 addition of the numbers in the binary form. Peers in the communication can determine only if it has the secret key with it. This ensures a secure communication between the communicating peers.

This key thus sent to both the peers could be used as a seed for the generation of some random number which can initiate the communication between the two parties.

The steps could be explained as shown below,

1. Peer A sends a request to CA along with k as k $\oplus$ h(a).

2. At the CA, k is rendered using the secret key of A
3. Generate binary sequence using Goldbach ellipse equation with k value.
4. n = a + b
5. d(even number) = n + random number.
6. One of the many partition pairs of m is selected say p and q.
7. Binary key is generated using the index p and q.
8. This binary key is sent to both A and B using their secret key a and b as

   h(a)⊕ key and h(b)⊕key respectively

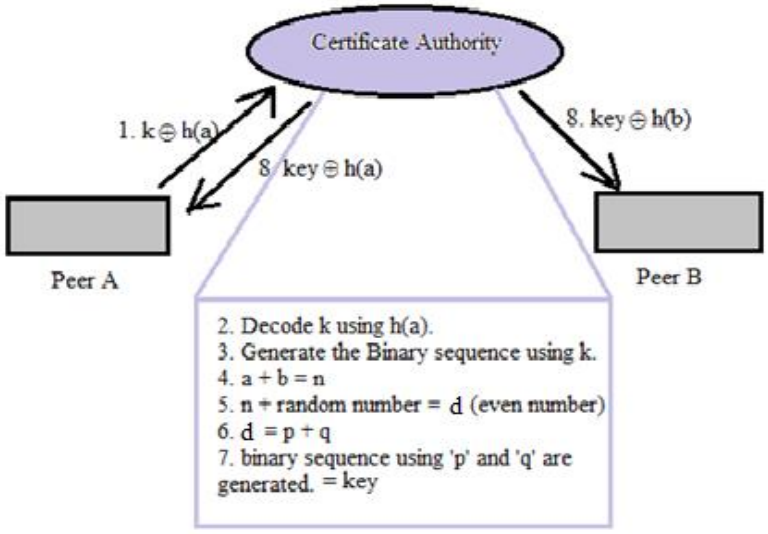

Figure14. Sequential execution of the protocol

Here, it is seen that the both the peers in the communication are unaware of the secret key of each other but are distributed the binary secret key safely.

Analysis

Goldbach partitions are partitions that are generated as a set of prime numbers and hence the secret binary key that is generated is dependent on the selected pair. For example if we consider the first 500 even numbers that is up to 1000, we see that the for an even number 1000, the Goldbach partitions ranges from (3, 997) to (491, 509). Hence, the binary key length varies from 997 to 18.

Table 11. Table showing the time to create Goldbach partitions

Number	Time to Encode(sec)
4	0.000003123
6	0.000002677
8	0.000002677
10	0.000006247
12	0.000010709
14	0.000008478
16	0.000024542

The time complexity to create the Goldbach partition is observed to be of the order of $O(n^2)$ but the time complexity to break the binary key will only be equal to $O(2^k)$, where

k is the length of the random number used in the first stage of the protocol. This is because, since the Goldbach partitions are created with the sequential search of two primes, the complexity of the program to create the partitions is of the order of $O(n^2)$.

When a graph is plotted with these values ranging up to 1000, we see that the time taken to calculate the Goldbach partition increases in the order of n^2. It is also seen that the maximum time taken for the largest number is less than a second. Hence, this shows that any Goldbach partition less than 1000 could be generated less than 0.01 seconds.

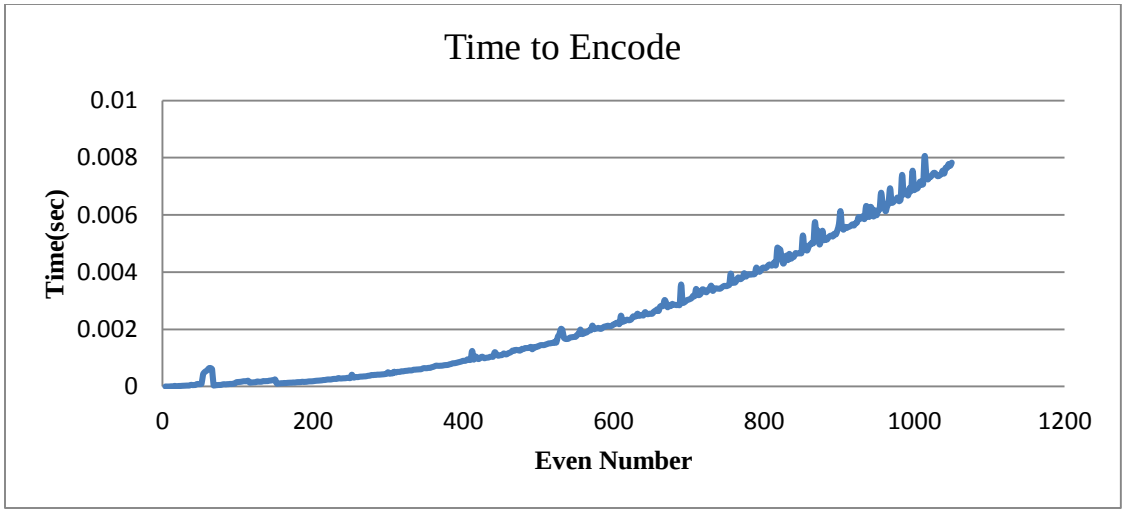

Fig 15. Graph showing the time required to create the Goldbach partitions.

But as mentioned before the complexity of the code for the eavesdropper would be related directly to the length of the random sequence used in the initial exchange. If the eavesdropper did not know the details of the system, then the complexity will increase to the length of the m sequence used in the latter part of the protocol.

Although the use of the partitions themselves do not lead to increased security, the partitions can be used as a kind of puzzle in devising other challenge-resolution cryptographic systems [3],[4].

CHAPTER V

CONCLUSION

This thesis presents a method of communicating keys using sequences obtained from the partitions of even numbers as primes, which is the Goldbach conjecture. We have investigated the randomness properties of these sequences. New variants of the prime partitions are examined and it is found that the sequences so obtained have excellent cross correlation properties. An algorithm is devised where the Goldbach partitions are used to exchange keys via a certification authority.

REFERENCES

[1] B. Schneier. Applied Cryptography: Protocols, Algorithms and source code in C. John Wiley & Sons, 1995.

[2] S. Kak, The piggy bank cryptographic trope. arXiv:1301.0313

[3] S. Singh, The Code Book: the Secret History of Codes and Code-breaking. Fourth Estate, London, 1999.

[4] S. Kak, On the method of puzzles for key distribution. Int. Journal of Comp. and Inf. Sciences 13: 103-109, 1984.

[5] S. Kak, A cubic public-key transformation. Circuits, Systems and Signal Processing 26: 353-359, 2007.

[6] A. Parakh and S. Kak, Online data storage using implicit security. Information Sciences 179: 3323-3331, 2009.

[7] A. Parakh and S. Kak, Space efficient secret sharing for implicit data security. Information Sciences 181: 335-341, 2011.

[8] S Kak, Information, physics and computation. Foundations of Physics 26: 127-137, 1996.

[9] S Kak, Quantum information and entropy. International Journal of Theoretical Physics 46:860-87, 2007.

[10] R. Landauer, The physical nature of information. Physics Letters A 217: 188-193, 1996.

[11] S. Kak, The information complexity of quantum gates. Int. J. of Theoretical Physics 45: 933-941, 2006.

[12] S. Kak, A three-stage quantum cryptography protocol. Foundations of Physics Letters 19: 293-296, 2006.

[13] M. Bellare and P.Rogaway, Provably Secure session key distribution: the three party case. Annual Symposium on the Theory of Computating, ACM 1995.

[14] M. Bellare, D. Pointcheval and P.Rogaway: Authenticated Key Exchange Secure Against Dictionary Attacks. Eurocrypt 2000 Proceedings Springer-Verlag 2000.

[15] A Kolmogorov, Three approaches to the quantitative definition of information. Problems of Information Transmission. 1:1-17, 1965

[16] S Kak, A Chatterjee, On decimal sequences. IEEE Transactions on Information Theory IT-27: 647-652,1981.

[17] S. Kak, Encryption and error correction coding using D sequences. IEEE Transactions on Computers C-34: 803-809, 1985

[18] S. Kak, New results on d- sequences. Electronics Letters 23: 617, 1987.

[19] L.R. Welch, Lower bound on Cross Correlation of signals. IEEE Trans on Information Theory IT-20: 397-399, 1974.

[20] R. Gold, Maximal Recursive sequences with 3 valued recursive cross correlation function. IEEE trans Inform. Theory IT-14: 154-156, 1968.

[21] V.M. Sidel'nikov, On mutual correlation of sequences. Soviet Math Doklady IT-12: 197-201, 1991.

[22] G.H. Hardy and J.E. Littlewood, Some problems of partitio numerorum; III: on expression of a number as a sum of primes, Acta Mathematica 44: 1- 70, 1922.

[23] J. M. Deshouillers, A. Granville, W. Narkiewicz and C. Pomerance, An upper bound in Goldbach's problem. Mathematics of Computation 61: 209-213, 1993.

VITA

KANCHU KRISHNAMA RAJU

Candidate for the Degree of

Master of Science/Arts

Thesis: SECURE KEY TRANSFER PROTOCOL USING GOLDBACH SEQUENCES

Major Field: Computer Science

Biographical:

Education:

Completed the requirements for the Master of Science/Arts in Computer Science at Oklahoma State University, Stillwater, Oklahoma in May, 2013.

Experience:

Professional Memberships: