Design of Spreading Sequence Based on Non Supersingular Elliptic Curve Points over Finite Fields for Security Applications

Saksham Sharma[1], Saravanan R[2]
[1]Senior Professor, [2]Dean
[12]Vellore Institute of Technology

Abstract- Use of Non-supersingular elliptic curve (EC) over Galois field F_2n with order nis explored in the present paper for designing spreading sequence generator, which addresses most of the drawbacks of the existing schemes available in the literature.The randomness of the generated sequence has been statistically analyzed using run test, matrix run test and one sample run test the proposed generator outperforms its contemporaries in terms of Mean Square Auto-correlation (MSAAC) and cross-correlation (MSACC) values.

Keywords- spreading sequence, elliptic curve, security.

I. INTRODUCTION

Spread spectrum modulation and CDMA (Code division multiple access) applicationsactively use spreading sequences [1-3].In cryptographic applicationslike speech and image encryption, spreading sequences having good correlation and randomness properties are preferred choice[4-6].

Various spreading sequences used for analysis as a part of literature survey are:

Sequences→ Properties ↓	M Sequence	WH Sequence	OVSF Sequence	Gold Sequence	Barker Sequence
Generation Technique	Using Linear shift register and Characterized by generator polynomial	Using Hadamard Square matrices	Rearranging Walsh functions using tree structure	Modulo -2 operation of two m- sequences	Subset of PN codes
Properties	Satisfy Run Property and are Spectrally flat	Orthogonal sequence but do not Satisfy Run property	Variable Orthogonal sequence	Satisfy Run & Balance Property	Satisfy Run & Balance Property
Property	Low Periodic Autocorrelation	Low Autocorrelation	Hamming Correlation	Low Periodic Crosscorrelation	Low Aperiodic Autocorrelation
Applications	Not suitable for speech encryption	No Multi access interference under perfect synchronization	Used as a channelization code in WCDMA forward and reverse link	As a scrambling code in WCDMA	Used for pulse compression in radar systems.

The proposed method of generating spreading sequences based on elliptic curve over Galois field possess better randomness properties and improved correlation values than the above mentioned spreading sequences based on the literature survey.

1. Proposed spreading sequence generator

- Consider $a_2 = z^3 and a_6 = z^3 + 1$

  The points which satisfy the elliptic curve

$$y^2 + xy = x^3 + z^3 x^2 + z^3 + 1$$

  are:

  (0011, 1100) (1000,0001) (1100,0000) (0001, 0000) (0011, 1111) (1000, 1001) (1100,1100)

The proposed spreading sequence is generatedby means of elliptic curve (EC) over Galois Fields.

- Consider the elliptic curve $y^2 + xy = x^3 + a_2x^2 + a_6$

  Specific values of a_6 can give maximum strength curves. $If a_2$ is 0 then the calculations are a touch faster. When a_2 is nonzero, the curve is called a twist.

(0001, 0000) (0101, 0000) (1001, 0110) (1111, 0100) (0001, 0001) (0101, 0101)(1001,1111) (1111,1011) (0010,1101) (0111,1011) (1011,0010) (0010,1111) (0111,1100) (1011,1001

- These pointsare coded using Galois Field F_2n. The polynomial $f(x) = x^4 + x + 1$ is a primitive polynomial over Galois Field. Then $x^4 = x + 1$. The identity $x^4 = x + 1$ is used repeatedly to form the polynomial representation for the elements of GF F_2n shown in Table 2.1

Table 2.1 Polynomial representation of elements of galois field.

$g^4 = 1 + g$	$g^5 = g + g^2$	$g^{10} = g^2 + 1 + g$	$g^{11} = g^3 + g + g^2$
$g^6 = g + g^3$	$g^7 = g^3 + 1 + g$	$g^{12} = 1 + g + g^2 + g^3$	$g^{13} = 1 + g + g^2$
$g^8 == 1 + g^2$	$g^9 = g + g^3$	$g^{14} = 1 + g^3$	$g^{15} = 1$

- Calculation of Trace function

The trace is a mapping from F_{2n} to F_2. Let the trace vector be represented as

$$T = t_{m-1}x_{m-1} + t_{m-2} \quad x_{m-2} + \; t_1 x + t_0$$

Starting at row g^0 and summing the values on the diagonal from bottom right and moving up to the left the trace function is calculated as,

$$t_0 = 1 \qquad t_1 = 0 \qquad t_2 = 0 \qquad t_3 = 0$$

- The points satisfying the elliptic curve are mapped into two bits by the trace function.
- To compute the Trace of g^{14} (1001) AND operation is carried out on the Trace vector (1000) and the number. Then SUM up the resulting bits. In this case, the trace of g^{14}(1001) modulo $x^4 + x + 1$ is 1. The trace value of the elements of Galois FieldF_2nis shown in Table 1.2.

Table 2.2 Trace Values of elements of Galois Field

Power representation	Trace Values	Power representation	Trace Values	Power representation	Trace Values
1	0	g^5	0	g^{10}	0
g	0	g^6	1	g^{11}	1
g^2	0	g^7	1	g^{12}	1
g^3	1	g^8	0	g^{13}	1
g^4	0	g^9	1	g^{14}	1

X-coordinate sequence: $\{\{a_i == TR\ (x_i)\}$= 100001100000…..

Y-coordinate sequence: $\{b_i == TR\ (y_i)\}$ = 110111001011.........

- Interleave (a_i, b_i):

$P = (a1; b1; a2; b2; \_\_\_ \; ; a32; b32)$

P = 11010001011100001000101…………

P is the generated spreading sequence

II. PERFORMANCE ANALYSIS OF EC BASED SPREADING SEQUENCE GENERATOR

The proposed sequence randomness has been tested using matrix run test, one sample run test, run test and correlation.

Matrix rank test: One of the standard randomness test available in the literature in time domain is the matrix rank test. Let p_0; p_1; :::; p_{r-1} be rconsecutivebinary digits from a PN sequence of length N = 2^n-1, wherer< N, which form the matrix

$$R = \begin{bmatrix} p_0 & p_1 & \cdots & p_{r-z} \\ p_1 & p_2 & \cdots & p_{r-z+1} \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

with n < z<r-2. Then rank(M) over GF(2) mustalways be less than z.

Considering r = 10, with n < z<r-2, let us consider z = 6. For the proposed spreading sequence in consideration

$$R = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

Rank of the above matrix is 5which is less than z and hence pass the test of randomness.

One sample run Test : One sample run test is used to find whether a sequence is truly random.

According to the run test if number of runs in a sequence lie between the lower and upper critical value for a given significance level then the sequence is said to be random.

Hypothesis H0 : Pattern of occurrences of ones and zeroes is truly a random process.

Hypothesis H1 : Pattern of occurrence of events is not random.

The sequence so generated by the proposed method

No : of Runs = 13

No: of ones n1 = 19

No: of zeroes n2 = 11

Considering critical value of level of significance α to be 0.05 for a two-sided test. The lower and upper critical values are determined from the table given by Bluman. Elementary statistics considering n1, n2 to be 19 and 11 respectively. According to Bluman the lower cut off is 9 and upper cutoff is 21. Therefore number of runs should lie between 9< R <21 for the sequence to be random. Since number of runs is 13,therefore it follows the hypothesis H0 that the sequence is random.

Run Test: This particular run test is used to find whether occurrence of each bit is independent of another.

Hypothesis Ho : Each bit is independent in the generated sequence

Hypothesis H1 : Each bit is not independent in the generated sequence

The sequence so generated is P = 1 1 1 1 0 1 1 1 1 1 0 0 1 1 1 1 1 0 0 1 1 0 1 0 0 0 1 0 0 1

Considering α = .05 , No : of ones n1 = 19, No : of zeroes n2 = 11 and number of runs R = 13

Expectation $E(R)=\frac{2n_1 n_2}{n_1+n_2}$ **= 11.92**

Variance $Var(R) = \frac{2n_1 n_2(2n_1 n_2 - n_2)}{(n_1+n_2)^2} = 6.174$

Region of Acceptance for hypothesis h0 is given by

$$E(R) - z_\rho\sqrt{Var(R)} \le R \le E(R) + z_\rho\sqrt{Var(R)}$$

Since level of significance α = .05 the value of z_ρ from the Table is 1.96. therefore

As calculated $7.06 \le R \le 16.78$

Since for the generated sequence R = 13 therefore it satisfies hypothesis Ho that bits so generated are independent.

Correlation Test: Aperiodic Correlation $r_{i,j}$, Mean square aperiodic auto correlation(MSAAC) and Mean squareaperiodic cross correlation(MSACC) measures[10] are used to measure the randomness of proposed binary sequence.Periodic autocorrelation function will measure the correlation of the sequence with a cyclic shift of its sequence.Oppermann and Vucetic [7] has introduced these correlation measures shown in Table 3.1

Table 3.1 Parameters for Correlation

Sr. No	Representation	Randomness Measure	Mathematical formula
1	$c_j(n)$ represents non-delayed version of $c_k(i)$, by 'τ ' units N is the length of the sequence c_i .	$r_{i,j}$	$r_{i,j} = \frac{1}{N}\sum_{\tau=1-N}^{N-1} c_i(n)c_j(n+\tau)$
2		MSAAC	$MSAAC = \frac{1}{M}\sum_{i=1}^{M}\sum_{\tau=1-N}^{N-1} \lvert r_{i,j}\rvert^2$
3		MSACC	$MSACC = \frac{1}{M(M-1)}\sum_{i=1}^{M}\sum_{j=1}^{M}\sum_{\tau=1-N}^{N-1} \lvert r_{i,j}\rvert^2$

Test Results and Comparative Analysis of Spreading Sequence Generator

The correlation test results on spreading sequence generator by means of elliptic curve (EC) over Galois Field are shown in Table 3.2

Table 3.2 Correlation measures for PN sequences of length 16 bits and 32 bits.

Sequences→ Properties ↓	M Sequence	WH Sequence	MWH Sequence	OVSF Sequence	Gold Sequence	Barker Sequence	Proposed Sequence
MSAAC(16bits)	0.3467	4.0625	1.8125	1.8125	--	--	0.245
MSACC(16bits)	--	0.7292	0.8792	0.8792	--	--	0.672
MSAAC(32bits)	0.4807	6.5938	3.2188	3.2188	0.6866	0.8127	0.6866
MSACC(32bits)	--	0.7873	0.8962	0.8962	0.7451	1.0505	0.7451

III. CONCLUSION

Applications likespread spectrum modulation and encryption techniques require spreading sequence generator with low computational time and good statistical randomness properties.The paper focuses on the application of properties of Finite fields and elliptic curves in the design of a spreading sequence. The run test and correlation test results on spreading sequence generator by means of elliptic curve (EC) over Galois fields are presented. The spreading sequence so generated possess reduced correlation and hence suitable for security applications.

IV. REFERENCES

[1]. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120–126, 1978.

[2]. M. Blum and S. Micali, "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits," SIAM Journal of Computing, Vol. 13, No.4, pp. 850-864, 1984.

[3]. L. Blum, M. Blum, and M. Shub, "A Simple Unpredictable Pseudorandom Number Generator," SIAM Journal on Computing, Vol. 15, No. 2, pp. 364–383, 1986.

[4]. Johan Håstad, Russell Impagliazzo, Leonid A. Levin and Michael Luby, "Construction of a Pseudo-Random Generator From Any One-Way Function" SIAM Journal of Computing, Vol.-28, pp.1364-1396,1999

[5]. Tai-Kuo Woo, "Orthogonal variable spreading codes for wideband CDMA," IEEE Trans. On Vehicular Technology, vol. 51, no. 4, pp. 700-709, July 2002.

[6]. N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, No. 177, pp. 203-209, 1987.

[7]. V. S. Miller, “Uses of Elliptic Curves in Cryptography,” Advances in Cryptology, CRYPTO'86, Lecture Notes in Computer Science, Vol. 218, pp.417-428, Springer 1986.

[8]. N.K. Pareek, V. Patidar, “A random bit generator using chaotic maps”, International Journal of Network security, Vol. 10, No1, pp. 32-38, 2010

[9]. Z. J. Shi, H. Yan, “Software Implementation of Elliptic Curve Cryptography”, International Journal of Network security, Vol.7, No1, pp.141-150, 2008.

[10]. L. Parameswaran and K. Anbumani, “Content based Watermarking for Image Authentication Using Independent Component Analysis” Proceedings of Informatica, pp. 299-306, 2008.

[11]. E. Martinian, B. Chen, and G.W. Wornell, “Information Theoretic Approach to the Authentication of Multimedia,” Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents III, San Jose, California, USA, Vol. 4314, pp. 185–196, 2001.

[12]. F. Cayre and P. Bas, Ker Kerckhoffs-based embedding security classes for woa data hiding. IEEE Transactions on Information Forensics and Security, Vol.3, No1, pp. 1-15, 2008

[13]. C.Y. Lin and S.F. Chang, “SARI: Self-Authentication-and Recovery Image Watermarking System,” Proceedings of ACM International Conference on Multimedia, Ottawa, Canada, Vol.9, pp. 628-629, 2003.

[14]. V. Milosevic, V. Delic and V. Senk, “Hadamard transform application in speech scrambling,” Proc. IEEE, Vol. 1, pp. 361-364, July 1997.

[15]. Tai-Kuo Woo, “Orthogonal variable spreading codes for wideband CDMA,” IEEE Trans. Vehicular Techn., vol. 51, No. 4, pp. 700-709, July 2002.

[16]. E. H. Dinan and B. Jabbari, “Spreading codes for direct sequence CDMA and wideband CDMA cellular networks,” IEEE Commun. Magazine, Vol. 36, No. 4, pp. 48-54, Sep. 1998.

[17]. Elementary statistics A Step-By-Step Approach, 8/e, Allan G. Bluman

[18]. Kai-Uwe Schmidt and Jürgen Willm, “Barker sequences of odd length,” International Journal on Designs, Codes and Cryptography, Volume 80, Issue 2, pp 409–414, Aug 2016.

[19]. João S. Pereira and Henrique J. A. da Silva, “ M-ary mutually orthogonal complementary gold codes,” proceedings of IEEE Signal Processing Conference, 2009.

[20]. Sujit Jos, Preetam Kumar and Saswat Chakrabarty, “ Performance Comparison of Orthogonal Gold and Walsh Hadamard Codes for Quasi-Synchronous CDMA Communication,” International Conference on Distributed Computing and Networking ICDCN 2009, pp 395-399.

[21]. X. Wang, Y. Wu and B. Caron, “Transmitter identification using embedded pseudo random sequences,” IEEE Tran. Broadcasting, Vol. 50, No. 3, pp. 244-252, Sep. 2004.

[22]. AbhjitMitra , On Pseudo-Random and Orthogonal Binary Spreading Sequences International Scholarly and Scientific Research & Innovation Vol.2, No:12, 2008

[23]. World Academy of Science, Engineering and Technology International Journal of Electronics and Communication Engineering Vol:2, No:12, 2008

[24]. Seberry, J. R., Wysocki, B. J. &Wysocki, T. A. (2005). Performance comparison of sequences designed from the Hall Difference Set and Orthogonal Gold Sequences of Length 32. In M. Blaum, R. Carrasco & M. Darnell (Eds.), International Symposium on Communication Theory and Applications (pp. 104-107). United Kingdom: HW Communications Ltd.

[25]. Lai phrakpam, Dolendro Singh, and KhumanthemManglem Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography,”Procedia Computer ScienceVolume 54, 2015, Pages 73-82, ElsevierUnder a Creativ India Eleventh International Conference on Image and Signal Processing, ICISP 2015, August 21-23, 2015, Bangalore, India

[26]. Elgamal Encryption using Elliptic Curve Cryptography Rosy Sunuwar, SurajKetanSamal CSCE 877 - Cryptography and Computer Security University of Nebraska- Lincoln December 9, 2015

[27]. Probabilistic data encryption using elliptic curve cryptography and Arnold transformationPublished in: I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 IEEE International Conference on , Feb. 2017

[28]. AnsahJeelaniZargar, MehreenManzoor and Taha Mukhtar, “Encryption/decryption using elliptical curve cryptography,” International Journal of Advanced Research in Computer Science Vol 8, No. 7, July – August 2017