INTERNET VOTING SYSTEM BASED ON MODIFIED ELLIPTIC CURVE CRYPTOGRAPHY

Kaustubh Pimparkar

Information Technology Department,

Vishwakarma Institute of Information Technology, Kondhwa, Pune

ABSTRACT

The election system is necessitating of every democracy and the administration formed is dependent on the results of the election. The election process paves the path for every voter to select a representative among themselves who can guide the democratic system towards the welfare of the society. The voting system has observed many effective changes over the past few decades, right from the traditional paper ballot voting to electronic voting and now towards the Internet Voting. However, the voter choice is a reliable and verifiable Voting where in manual system he used to stamp on the symbol of his choice. This requires a security algorithm that could resist the attacks and keep the data confidentiality and also authenticate Voter in online. Modified Elliptic Curve Cryptography is used for both confidentiality and authentication.

Keywords: Internet Voting (I-Voting), electronic voting, authenticate Voter, Modified Elliptic Curve Cryptography (MECC), Parallel Multicore Particle Swarm Optimization (PMPSO)

I. INTRODUCTION

Voting is the mechanism used by any eligible voter to option his choice from a list of candidates. Elections are conducted everywhere from small union election in order to select a leader to huge general elections to select the prime minister or president. This is used everywhere such as school representatives, college representatives, union leader, national or state leader. Voting is required to be conducted in various situations [1, 2].

Where ever election systems are conducted, the election system must be robust and secure which should resist a variety of fraudulent actions. This is required to be transparent and comprehensible that voters and candidates should accept the results of the election without any issue. However, when we refer to previous contexts, some cases have immense effect on conducting the election smoothly and had influence on the result that is unacceptable. A secured voting system has to meet the following criteria [3].

1. There are some attacks from manipulated persons which include ballot stuffing and incorrect counting by few persons inside counting center.
2. Secrecy of ballot is important and it should guarantee the voter safety which has no evidence showing to which candidate vote is casted by the voter.
3. The system should be flexible and understandable by all kinds of voters. Every voter should be able to cast his vote either aged or disabled.
4. The overall voting process should be fair and effective and voter should feel that the entire system is genuine.
5. Authentication of voter is must as the right person should cast the vote.

6. Speed and Accuracy are also important in achieving secure voting.

As the role of Internet voting system is crucial, it is difficult to come up with a system which is highly secure & accurate in all senses. If these factors of security are satisfied, then Internet voting could be a great option over paper systems and EVMs.

II. MODIFIED ELLIPTIC CURVE CRYPTOGRAPHY

Parallel Multicore Particle Swarm Optimization (PMPS0):

The particle swarm optimization based on the evolutionary technique of computation that optimizes an objective function by performing population-based search. The particles in population that are potential solutions are similar to birds in a flock. The particles are first initialized randomly and then fly across the multi-dimensional search space. Every particle updates its velocity and position based on its own best experience and that of the entire population. The updating policy will cause the particle swarm to move toward a region with a higher object value [5].

Parallel Multicore processing aims to produce the same results by using multiple processors that ultimately increases the CPU utilization [6]. In this study, the spirit of the data parallelism method was utilized to create a parallel particle swarm optimization (PPSO) algorithm. The purpose of applying parallel processing to particle swarm optimization goes further than merely being a hardware accelerator. Rather, a distributed formulation is developed which gives better solutions with reduced overall computation. It is difficult to find an algorithm which is efficient and effective for all types of problems. Our research has indicated that the performance of PPSO can be highly dependent on the level of correlation between parameters and the nature of the communication strategy. In PMPSO the particles update its velocity and position by using the following equation which denotes k_{th} iteration with n cores. The mathematical form of the parallel particle swarm optimization algorithm can be expressed as shown in equation (1) and (2) [7].

$$\begin{aligned} V_{1,n}^{k+1} &= wV_{1,n}^{k} + F_1 \times r_1 \times \left(P_{best,n} - U_{1,n}^{k}\right) \\ &\quad + F_2 \times r_2 \times \left(G_{best} - U_1^{k}\right) \qquad (1) \\ U_{1,n}^{k+1} &= U_{1,n}^{k} + V_{1,n}^{k+1} \quad \ldots \qquad (2) \end{aligned}$$

Here $V_{1,\ nk}$ represents the Velocity of agent at k_{th} iteration at n_{th} core and $V_{1,\ nk+1}$ at next iteration. $U_{1,\ nk}$ is the current position of the agent at k_{th} iteration at n_{th} core and $U_{1,\ nk+1}$ at next iteration. G_{best} is the best position among all particles from the first to last iteration basing on the number of cores which are dependent upon system being executed. The complete algorithm for PMPSO is given below and the figure 1 depicts the flowchart.

Step 1 : Initialize each particle

Step 2 : Repeat step 1 until all particles are initialized

Step 3: Calculate Fitness value for each particle applying

multicore parallel processing.

Step 4 : Check if fitness value is better than particles personal best value in each core

Step 5 : Set particles best value as current pbest.

Step 6 : Calculate parallel personal best ppbest.

[End of Step4 if statement]

Step 7 : Repeat Step 3 thru 6 until all particles are calculated.

Step 8 : Select gbest (global best) with the best fitness value among all particles

Step 9 : Update velocity of each particle by using equation 7.

Step 10 : Update position of each particle by using equation 8.

Step 11 : Repeat Step 6 and 7 until all particles are updated.

Step 12 : Repeat Step 2 thru 8 until minimum error or maximum iterations

Advantages of PMPSO:

1. Easy to Implement and simple
2. Attains solution faster.
3. Applied to Engineering and also Scientific Problems as this is based on intelligence.
4. Compared to GA this has no overlapping and mutation calculation. Search is based on calculating the velocity of particle.
5. Uses real number code and the number of dimensions are equal to constant of solution.
6. Effectively utilizes processor capabilities.

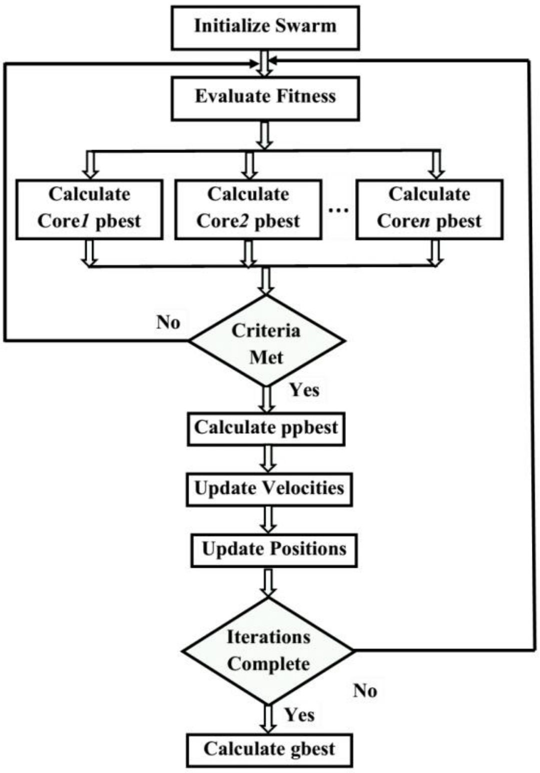


Figure 1: Muticore Parallel PSO Flowchart

Modified ECC:

Here ECC and PMPSO are combined where the parameters in ECC are chosen by using PMPSO. This uses the concepts of public key cryptography that involves both private and public keys and elliptic curve. The private keys are chosen by optimization algorithm PMPSO.

MECC Discrete Logarithm problem:

When P and Q are known, find k such that Q=kP. This problem is known as the discrete logarithm problem for elliptic curves which is believed to be a "hard" problem, in that there is no known polynomial time algorithm that can run on a classical computer[8]. DLP is also available in other cryptosystems such as the Digital Signature Algorithm (DSA), ElGamal algorithm and the Diffie-Hellman key exchange (DH) [9]. . However in

ECC the discrete logarithm problem for elliptic curves seems to be harder if compared to other similar problems used in cryptography. This implies that we need fewer bits for the integer k in order to achieve the same level of security as with other cryptosystems [9, 10]. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 3 (2016) pp 1874-1878 © Research India Publications. http://www.ripublication.com 1876

Authentication with MECC:

The authentication using MECC is as shown in below procedure.

1. Two users A and B select the elliptic curve parameters.
2. Admin B takes a random point Message Point, MP on the selected elliptic curve which is transmitted to Voter.
3. Voter A selects his private key P_{rA} using PMPSO algorithm which is kept securely with him.
4. Voter computes his public key point by using his private key and applying scalar multiplication on elliptic curve point MP basing on equation 3 and sends to Admin

$$P_{uA} = P_{rA} \text{ x } MP \qquad \ldots(3)$$

5. Similarly, Admin selects his private key using PMPSO algorithm P_{rB} that is kept securely with user B.
6. User B computes his public key point using his private key and based on equation 4 and sends to User A

$$P_{uB} = P_{rB} \text{ x } MP \qquad \ldots(4)$$

7. Admin computes final point basing on equation 5

$$P_a = P_{rA} \text{ x } P_{uB} \qquad \ldots(5)$$

8. Voter computes final point basing on equation 6

$$P_b = P_{rB} \text{ x } P_{uA} \qquad \ldots(6)$$

9. This implements the concept of shared secret key as shown in equation 7

$$P_a = k_aR = k_ak_bP = k_bk_aP = k_bQ = P_b \qquad \ldots(7)$$

Encryption with MECC:

1. Voter selects his private key his private key using PMPSO algorithm which is any random number P_{ra}.
2. Then he computes his public key from private key and sends that to Admin basing on equation 8 and which is another point on elliptic curve.

$$Q = nP_b \qquad \ldots(8)$$

3. Voter signs with private key
4. Admin checks if he is valid voter and he sends his public key P_{uA} to voter.
5. Voter encrypts his vote using the admin's public key P_{uA}.
6. Admin decrypts the voter's choice using his private key P_{rA}.

MECC Advantages:

Compared to traditional systems, MECC algorithms have following advantages [12, 13]

1. Short Keys
2. Quick Processing
3. Same curve can be used for several distinct key pairs.
4. Used to factor integers
5. Ensures Integrity, Authentication and Confidentiality

Reliable and Verified Internet Voting System using MECC

The Reliable Internet voting is possible by applying the following procedure.

1. Authenticate Voter by using ECC
2. Encrypt Vote by using MECC
3. Verify Vote by applying the procedure given below.

Voter may like to verify the vote whether it is transmitted correctly and his choice is correctly counted. This requires a mechanism where the voter is authenticated and encrypted vote is send to voter which is decrypted by using his private key [14, 15].

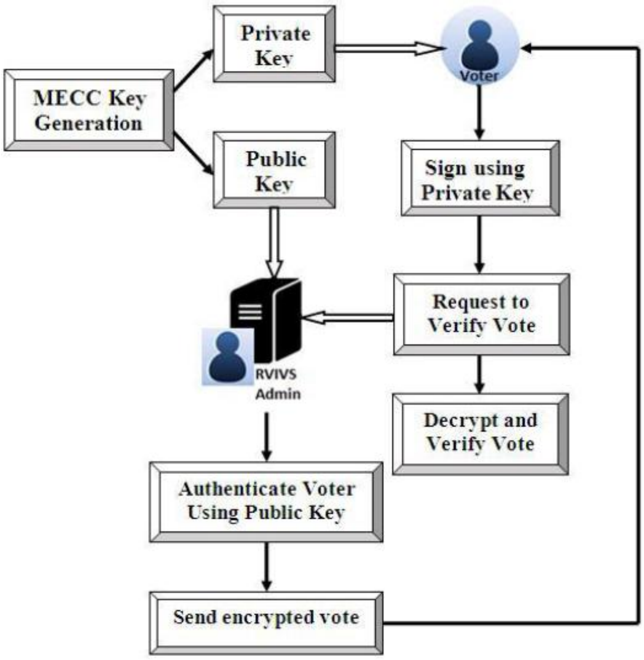


Figure 2: Verifiable Vote

Voter chooses his private key which is any random number n_v. Then he computes his public key from private key and sends that to Admin elliptic curve. Voter signs with private key and Admin checks if he is valid voter and he sends public key to voter. Voter requests to verify his vote. Admin encrypts vote using the voter's public key. Voter decrypts vote using his private key to verify that his vote is counted to the candidate of his choice [16, 17].

III. RESULTS

To maintain the security of the system, the voter has to take the responsibility in keeping his private key secure. The channel also should be secure while transmitting the keys, so many times hashing and encryption algorithms is applied to the private key to ensure non-repudiation and integrity. The proposed algorithm is developed and is tested on a case scenario. In this case the chosen elliptic curve is plotted in Fig 3.

Then authentication is applied and the table 1 shows the ECC results. Here MP is the Message Point and P_{rA} the private key of A and P_{rB} the private key of B. P_{uA} and P_{uB} are public keys of A and B computed from private keys using ECC operations. PA and PB are computed at both the ends using ECC operations to check for authentication which always same. However, it can be observed that PA and PB are sometimes reaching infinite values in ECC operations as they are going beyond the range.

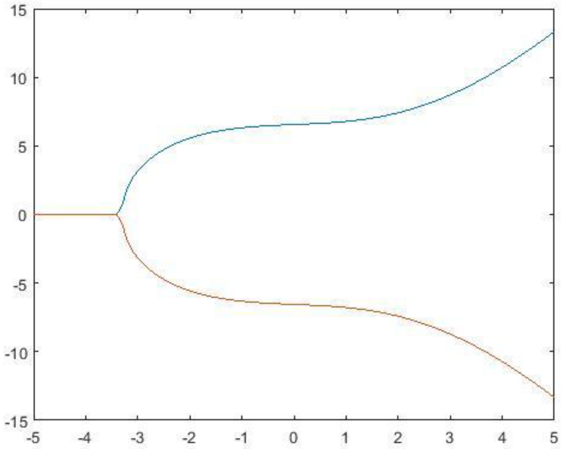
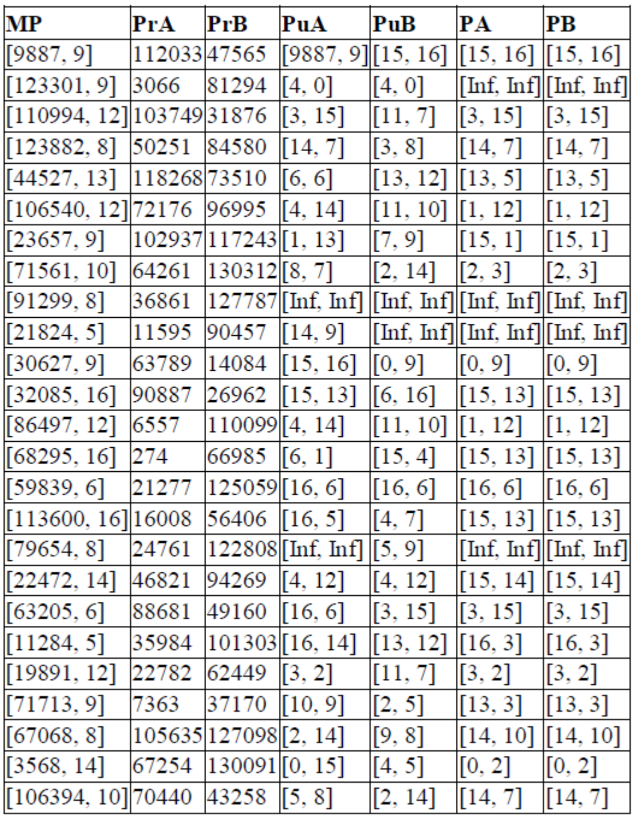


Figure 3: $x_3+2x+43$

Table 1: Authentication Parameters of ECC on x^3+2x+43 mod 17



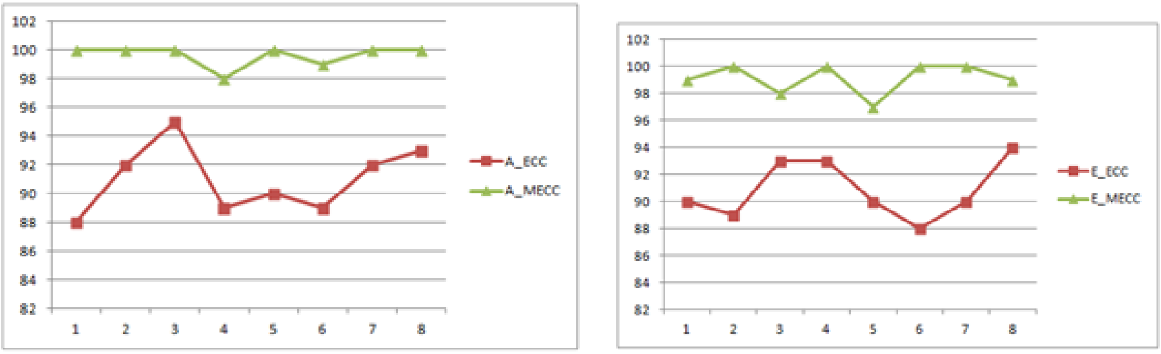
MP	PrA	PrB	PuA	PuB	PA	PB
[9887, 9]	112033	47565	[9887, 9]	[15, 16]	[15, 16]	[15, 16]
[123301, 9]	3066	81294	[4, 0]	[4, 0]	[Inf, Inf]	[Inf, Inf]
[110994, 12]	103749	31876	[3, 15]	[11, 7]	[3, 15]	[3, 15]
[123882, 8]	50251	84580	[14, 7]	[3, 8]	[14, 7]	[14, 7]
[44527, 13]	118268	73510	[6, 6]	[13, 12]	[13, 5]	[13, 5]
[106540, 12]	72176	96995	[4, 14]	[11, 10]	[1, 12]	[1, 12]
[23657, 9]	102937	117243	[1, 13]	[7, 9]	[15, 1]	[15, 1]
[71561, 10]	64261	130312	[8, 7]	[2, 14]	[2, 3]	[2, 3]
[91299, 8]	36861	127787	[Inf, Inf]	[Inf, Inf]	[Inf, Inf]	[Inf, Inf]
[21824, 5]	11595	90457	[14, 9]	[Inf, Inf]	[Inf, Inf]	[Inf, Inf]
[30627, 9]	63789	14084	[15, 16]	[0, 9]	[0, 9]	[0, 9]
[32085, 16]	90887	26962	[15, 13]	[6, 16]	[15, 13]	[15, 13]
[86497, 12]	6557	110099	[4, 14]	[11, 10]	[1, 12]	[1, 12]
[68295, 16]	274	66985	[6, 1]	[15, 4]	[15, 13]	[15, 13]
[59839, 6]	21277	125059	[16, 6]	[16, 6]	[16, 6]	[16, 6]
[113600, 16]	16008	56406	[16, 5]	[4, 7]	[15, 13]	[15, 13]
[79654, 8]	24761	122808	[Inf, Inf]	[5, 9]	[Inf, Inf]	[Inf, Inf]
[22472, 14]	46821	94269	[4, 12]	[4, 12]	[15, 14]	[15, 14]
[63205, 6]	88681	49160	[16, 6]	[3, 15]	[3, 15]	[3, 15]
[11284, 5]	35984	101303	[16, 14]	[13, 12]	[16, 3]	[16, 3]
[19891, 12]	22782	62449	[3, 2]	[11, 7]	[3, 2]	[3, 2]
[71713, 9]	7363	37170	[10, 9]	[2, 5]	[13, 3]	[13, 3]
[67068, 8]	105635	127098	[2, 14]	[9, 8]	[14, 10]	[14, 10]
[3568, 14]	67254	130091	[0, 15]	[4, 5]	[0, 2]	[0, 2]
[106394, 10]	70440	43258	[5, 8]	[2, 14]	[14, 7]	[14, 7]

Table 2 shows the MECC resultant data. Parameters are similar as specified in table 1. However, the values in elliptic curve are optimized using PMPSO. Hence it is clearly observed that PA and PB are always within the range.

Table 2: Authentication Parameters of MECC on $x^3+2x+43 \bmod 17$

MP	PrA	PrB	PuA	PuB	PA	PB
[126896, 10]	100547	33889	[15, 6]	[4, 1]	[12, 10]	[12, 10]
[78205, 8]	45121	86131	[5, 9]	[5, 8]	[5, 9]	[5, 9]
[13374, 10]	14551	69401	[6, 15]	[6, 2]	[8, 10]	[8, 10]
[67966, 9]	47881	125201	[67966, 9]	[67966, 9]	[67966, 9]	[67966, 9]
[76929, 13]	78163	51461	[8, 9]	[4, 4]	[8, 8]	[8, 8]
[24014, 9]	117979	25457	[7, 9]	[24014, 9]	[7, 9]	[7, 9]
[80001, 6]	20357	80671	[16, 11]	[16, 6]	[16, 11]	[16, 11]
[39398, 8]	128393	89563	[9, 8]	[9, 8]	[9, 8]	[9, 8]
[97862, 9]	87359	85847	[10, 8]	[1, 4]	[1, 13]	[1, 13]
[68669, 16]	1733	27077	[15, 4]	[15, 4]	[16, 5]	[16, 5]
[11980, 10]	6779	97021	[4, 16]	[12, 10]	[4, 16]	[4, 16]
[123565, 8]	953	3673	[5, 8]	[9, 9]	[5, 9]	[5, 9]
[31361, 5]	81637	92623	[16, 3]	[6, 6]	[13, 5]	[13, 5]
[43128, 6]	123979	163	[16, 6]	[16, 6]	[16, 6]	[16, 6]
[9838, 10]	75553	116483	[15, 6]	[8, 7]	[6, 15]	[6, 15]
[27157, 10]	49999	90437	[15, 11]	[6, 15]	[4, 16]	[4, 16]
[12183, 2]	11549	80909	[11, 15]	[15, 4]	[15, 13]	[15, 13]
[53013, 9]	59581	80809	[10, 8]	[15, 1]	[1, 4]	[1, 4]
[74615, 4]	109397	117619	[7, 15]	[16, 1]	[2, 13]	[2, 13]
[20567, 10]	10177	32299	[5, 9]	[2, 14]	[9, 8]	[9, 8]
[31545, 9]	93323	48527	[7, 9]	[10, 8]	[7, 8]	[7, 8]
[71559, 16]	104831	113417	[6, 16]	[11, 2]	[11, 2]	[11, 2]
[62709, 5]	112459	117361	[6, 6]	[13, 5]	[6, 6]	[6, 6]
[98065, 8]	2143	47441	[14, 7]	[14, 7]	[5, 9]	[5, 9]
[58245, 8]	70891	86453	[9, 9]	[9, 8]	[5, 8]	[5, 8]

This is similar in case of algorithm applied in authentication and encryption success rate is always high in MECC compared to ECC. The figure 4 shows the test results on both algorithms. The observations depict that both algorithms related to authentication and encryption using MECC are always highly accurate compared to those using ECC.



(a) Authentication using ECC and MECC (b) Encryption using ECC and MECC

Figure 4: Authentication and Encryption and Success Rate on test sets

IV. CONCLUSION

Voting is the process required whenever there is more than one person competing for any position or statements or views to be chosen among multiple choices. The voting system is improving step by step; advancement in the new system eliminates the drawbacks of the previous system. Every system tries to overcome the loop holes of the previous system. The proposed security algorithm is highly accurate in both the cases authentication and confidentiality. However security is not limited to an application and hence this can be extended to applications wherever there is requirement of integrity, confidentiality and authentication. Other optimization techniques can also be used to optimally choose the private keys in ECC.

REFERENCES

[1] Daniel Barbara and Hector Garcia-Molina, “The Reliability of Voting Mechanisms”, IEEE, vol. c-36, pp. 1197-1208, (1987).

[2] Behrooz Parhami, “Voting Algorithms”, IEEE, vol 43, No 4, pp. 617-629, (1994).

[3] Orhan Centinkoya, “Analysis of Security Requirement of Cryptographic Voting Protocols(Extended Abstract)”, IEEE, pp. 1451-1456, (2008).

[4] K. Sujatha, P. V. Nageswara Rao, A. Arjuna Rao, L. V. Rajesh, V. Vivek Raja; “Secured Internet Voting System based on Combined DSA and Multiple DES Algorithms”, ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II Advances in Intelligent Systems and Computing Volume 249, 2014, pp 643-650.

[5] J. Kennedy and R. Eberhart, “Particle swarm optimization, ” Proceedings of: IEEE International Conference on Neural Networks, Perth, WA, Australia, 1995, pp. 1942-1948.

[6] Sujatha, K. ; Nageswara Rao, P. V. ; Rao, A. A. ; Sastry, V. G. more authors “Multicore Parallel Processing Concepts for Effective Sorting and Searching”, Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on 2-3 Jan. 2015, IEEE, pp 162 – 166.