





## Enhancing Security in Online Voting Systems: A Cryptographic Approach Utilizing Galois Fields

Chittibabu Kandikatla<sup>1</sup>, Sravani Jayanti<sup>2</sup>, Pragathi Chaganti<sup>1</sup>, Hari Kishore Rayapoodi<sup>1,3</sup>,  
Chandra Sekhar Akkapeddi<sup>1</sup>

<sup>1</sup> Department of Mathematics, GITAM, Visakhapatnam 530045, India

<sup>2</sup> Department of Engineering Mathematics, College of Engineering, KLEF, Vaddeswaram 522302, India

<sup>3</sup> Department of Mathematics, Vasavi College of Engineering, Hyderabad 500031, India

Corresponding Author Email: [cakkaped@gitam.edu](mailto:cakkaped@gitam.edu)

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/mmep.110125>

### ABSTRACT

**Received:** 10 May 2023

**Revised:** 25 August 2023

**Accepted:** 10 September 2023

**Available online:** 30 January 2024

#### Keywords:

*cryptography, Galois field, group codes, key generation, online voting*

Ensuring information security is indispensable during data communication among a collective of entities. This requirement is exemplified in the context of online voting systems (OVS), which necessitate the conduction of fair and transparent elections. A pivotal aspect of securing the OVS involves authenticating authorized voters prior to vote casting and encrypting the votes before their transfer over a secure channel for tallying. The present study centers on the development of a mathematical model for an authentication scheme that can be implemented in an OVS to facilitate impartial elections. The devised model integrates mathematical and cryptographic principles of Galois fields, group codes, and pseudo-random key stream generators to formulate individual voter passcodes, thereby providing two-factor authentication. The proposed scheme is exemplified through a scenario suitable for orchestrating a medium-scale election involving 65,536 voters via an OVS. Furthermore, with the appropriate selection of inputs, the model exhibits the capacity to support large-scale elections.

## 1. INTRODUCTION

Cryptology is the study of developing cryptosystems and methods to crack the designed cryptosystems. Algorithms are designed to encrypt and decrypt information, exchange keys used for encryption and decryption, generate keys and hack the cryptosystem designed [1]. These algorithms are developed from the concepts of mathematical sciences such as finite fields, modular arithmetic, matrices etc. and are implemented using the programming languages [2]. The security, time and space complexity of the developed algorithm is of main concern in applying it in real time. The security of a cryptosystem is mainly constituted in the cryptographic key used to encode data and retrieve it. To safeguard the cryptographic key accountable for the security, several key exchange protocols are developed depending upon the number of communicating parties. These protocols ensure the safe key transfer over communication channels. But most of the key exchange protocols are prone to the Man-In-The-Middle attack which can be eradicated by providing user authentication.

One of the practical scenarios where user authorization and authentication are necessary is Election. Election is a fair process of electing a candidate based on the number of votes casted in favour. This process was manually conducted in ancient times. Electronic Voting Machines are invaded over time to facilitate elections by conducting them in short duration achieving total secrecy. With further onset of

technology concerning human comfort, online voting systems are designed which overcome congestion at polling booths and support remote voting. Internet voting is implemented for small scale elections [3] but the need for an efficient protocol which could be practically implemented for large-scale elections is prevalent.

A Voting System includes three major steps: Registration of voters, Vote Casting and Counting. The initial step of a voting system assures that no unauthorized voter casts the vote. Subsequently, votes are casted by the authorized voters at the polling booth which are stored in secret ballots. Finally, the encrypted votes are transferred to the counting officer over a secure channel for results. The entire framework of a secure Voting system is designed to achieve total secrecy and individual, eligible and universal verifiability [4, 5]. Internet Voting apply mathematical algorithms in software to establish the framework of a voting system [4, 6].

Porkodi and Sangavai [7] studied secure e-voting scheme over Circulant matrices is developed assuming the authenticity of the votes casted by the authorized voters. Falkner [8] et al. studied the initialization phase of registration operates a Pseudo Random Key Stream Generator (PRKG) to generate passwords for designing individual secret QR codes for voters. These QR Codes are employed by the voters to participate in the elections.

A Pseudo Random Key Stream (PRKS) is a sequence of numbers produced by a mathematical algorithm with an input seed value. A PRKS is periodic after certain time and an

adversary could guess the key stream with the knowledge of the input seed value. Our aim of this paper is to develop an authentication scheme which provides two-factor authentication and overcome the threat of a PRKG. The scheme applies an efficient cryptographic technique inspired from Amiruddin et al. [9] and Verma and Jain [10] to generate multiple keys for voters which authorize them to vote and retain the authenticity of the voter. The authentication scheme supports the registration phase of an online voting system which supports medium to large scale elections.

Amiruddin et al. [9] found that key generation techniques are proposed whose performance is measured by testing the algorithm for its key generation speed, key randomness, periodicity and complexity of the algorithm. Verma and Jain [10] studied Reed Solomon codes and parity check matrices are used in correcting passwords that are entered incorrect by the user with minute error. The designed method prompts the user with the correct password characters by retaining the security. In Cody Planteen [11], a method is proposed to develop a cryptographic key using the biometric fingerprints of a user.

The proposed authentication scheme in this paper is procured through the following mathematical and cryptographic concepts:

### 1.1 Galois field $GF(2^m)$

A Galois field is a field which has finite number of elements whose order is either a prime or a prime power. The elements of a Galois field  $GF(2^m)$  can be identified as polynomials of a maximum degree of  $(m - 1)$  or group of  $m$  bits which comprises of either 0s or 1s. When the elements are in the form of polynomials in  $GF(2^m)$  over a chosen irreducible polynomial of degree  $m$ , the field operations are addition modulo 2 and multiplication modulo 2. Due to the modulo 2 operations performed, the polynomials can be mapped to the group of binary bits. In Galois field  $GF(2^m)$ , the chosen irreducible polynomial of degree  $m$  plays an important role in identifying the elements of the field. With the change in the chosen irreducible polynomial, the mapping of polynomials with their equivalent group of  $m$  bits consisting of 0s and 1s differ [12, 13].

### 1.2 Subfields of $GF(2^m)$

A subset of Galois field  $GF(2^m)$  is its subfield if it is a field with respect to the same operations. The order of a subfield of  $GF(2^m)$ , is necessarily a power ( $n$ ) of 2 where  $n$  divides  $m$ . Thus, the total number of subfields of a field of order  $2^m$  is equal to the number of positive divisors of  $m$ . The subfield of  $GF(2^m)$  can be constructed by means of a primitive element of  $GF(2^m)$ . In the section 3 of this paper, the subfields of a Galois field  $GF(2^8)$  are constructed [12, 13].

### 1.3 Group codes

A group code  $B^a$  is a collection of block codes which forms a subgroup of an abelian group  $B^b$  where  $a < b$  and order of  $B^a = 2^a$ . An encoding function is a mapping from  $B^m$  to  $B^n$  where  $m < n$ . The set comprising of all the elements of  $B^m$  which are mapped to the elements of  $B^n$  forms a group with respect to XOR operation if the last  $(n - m) \times (n - m)$  sub matrix of the parity check matrix of order  $m \times (n - m)$

chosen is an identity matrix [13].

The rest of the paper is organized as follows: Section 2 presents the methodological approach of the proposed authentication scheme for OVS. Section 3 illustrates the proposed scheme through an example and describes its application in OVM. Section 4 covers the detailed analysis of the proposed scheme by describing its security aspects and implementation in medium scale elections. Section 5 concludes the presented work by highlighting its uniqueness, merits and applications.

## 2. PROPOSED AUTHENTICATION SCHEME FOR AN ONLINE VOTING SYSTEM

In a fair Internet Voting, votes casted by the authorized candidates are valid. Hence, to provide authorization to the candidates an initial step of registration of voters is performed before contesting the election online. During registration, a pass code framer can be used to generate a unique pass code for each candidate against the input ID of the individual. The created ID pass code combination serves as the authentication tool while casting the vote. Thus, while voting only the authorized candidates could cast vote and the validation of the casted vote is achieved through authentication.

Initially, this paper proposes a pass code framer which is designed applying mathematical and cryptographic techniques to generate multiple keys/pass codes against individual inputs by different users. Further, an authentication scheme employing the proposed pass code framer is developed which is implemented in an OVS to authorize and authenticate voters.

### 2.1 Pass code framer

The methodological approach to generate pass code is:

Step 1: Consider a Galois Field  $GF(2^a)$  with an irreducible polynomial of degree  $a$  (private to the system/central authority (CA)).

Step 2: Calculate the number of proper subfields ( $q$ ) of the chosen Galois Field and their elements. The total number of non-repeating elements in  $q$  subfields is  $l$ .

Step 3: Define an encoding function  $e: B^a \rightarrow B^b, b > a$  which maps the elements of  $B^a$  with some elements of  $B^b$  using a parity matrix  $P$  of order  $(b - a) \times a$ . (Private to the CA).

Step 4: Corresponding to  $l$  distinct elements of  $q$  subfields,  $l$  different pass codes are generated with respect to a single parity check matrix.

The pass code generation technique is explained through the pseudo code:

Parameters:

- Number of digits in the pass code (chosen by the system):  $k$

- Number of possible parity matrices:  $l$

Inputs to generate pass code: For  $i = 1, 2, \dots, l$ ,

- No. of 0s in the code word of  $B^b$  to which an element of the subfields of  $B^a$  is mapped:  $a[i]$  (private to the booth).

- No. of 1s in the code word of  $B^b$  to which an element of the subfields of  $B^a$  is mapped:  $b[i]$  (private to the booth).

- Prime number greater than  $k$  input by the voter:  $c[i]$  (private to the voter) // to support non-repetition of digits in the pass code.

Output:

- Array to store the obtained key/pass code values corresponding to a booth:  $K[k][l]$

### 2.1.1 Pass code generation

The pseudo code to generate pass code values is:

```

Start
for i = 1 to l
{
Input c[i]
K[1][i] = a[i] % c[i]
K[2][i] = b[i] % c[i]
for j = 3 to k
{
K[j][i] = {K[j-2][i]K[j-1][i] + j}%c[i]
}
}
End

```

The distinct users input and pass code combinations generated for multiple voters are:

$$(c[i], K[i][j]) \text{ for } i = 1, 2, \dots, k, j = 1, 2, \dots, l \quad (1)$$

#### Example:

For a single voter with input values,  $k = 5, c[1] = 7, a[1] = 2, b[1] = 3$ , the obtained stream values would be:  
 $K[1][1] = 2\%7 = 2$   
 $K[2][1] = 3\%7 = 3$   
 $K[3][1] = (2^3 + 3)\%7 = 4$   
 $K[4][1] = (3^4 + 4)\%7 = 1$   
 $K[5][1] = (4^1)\%7 = 4$   
The pass code is: (7, 23414)

However, the input by the voter can be taken in the form of fingerprints or unique Voter IDs. The proposed pass code framer requires a prime number greater than  $k$  as a user input. An algorithm could be applied essentially to convert the input by the voter to the required prime number.

### 2.2 Deployment of pass code framer in the authentication scheme for OVS

In an OVS, voter needs to be authorized to cast vote. The voter is authorized by assigning a unique ID and pass code combination. This combination is used to authenticate the voter before vote casting. The proposed mathematical model of authentication scheme employing pass code framer is:

Consider a Galois field  $GF(2^a)$ . The total number of elements in the proper subfields of  $GF(2^a)$  is  $l$ . Consider an encoding function  $e: B^a \rightarrow B^b$  as described in step 3 of section 2.1. The total number of parity matrices is  $2^{((b-a)(2a-b))}$ .

Each distinct element of the subfields is mapped with a unique element of  $B^a$  which is private to the booth. Therefore, maximum number of booths possible =  $l$ .

Different pass codes are generated corresponding to distinct elements of subfields and the chosen parity matrix. Therefore, maximum number of voters in a single booth = number of parity matrices =  $2^{((b-a)(2a-b))}$ .

Each voter is assigned a single booth where the private key of the booth is a codeword of  $B^a$  which is mapped to a unique codeword in  $B^b$ . The codeword in  $B^b$  is converted to its

decimal form which serves as the first part of the pass code.

The input by the voter:  $c[i]$ , number of 0s in the codeword of  $B^b$  of the specified booth:  $a[i]$ , number of 1s in the codeword of  $B^b$  of the specified booth:  $b[i]$ , is fed to the pass code framer which yields the pass code  $K[i][j]$ .

The pass code ( $c[i], P1, P2$ ) comprises of two segments  $P1, P2$ , where,

$c[i]$ =Voter ID,  
 $P1$ =Decimal equivalent of the codeword in  $B^b$  and  
 $P2=K[i]$ .

The first part of the pass code is verified by converting the decimal value to its equivalent binary value which is further decoded to retrieve the codeword in  $B^a$  (private key of the booth) by dropping the last  $(b - a)$  bits of the codeword in  $B^b$ .

The second part of the pass code is verified by matching the pass code-Id combination stored in the vault.

### 3. IMPLEMENTATION OF THE PROPOSED AUTHENTICATION SCHEME IN AN ONLINE VOTING SYSTEM

The proposed method is implemented through the example below:

Step 1:

Consider a Galois Field  $GF(2^8)$  with an irreducible polynomial  $x^8 + x^4 + x^3 + x^2 + 1$ . The total number of elements in  $GF(2^8)$  is 256. Let  $\alpha$  be the root of the polynomial  $x^8 + x^4 + x^3 + x^2 + 1$ . Since the powers of  $\alpha$  generate all the elements of  $GF(2^8)$  and its order is 255 therefore  $\alpha$  is the primitive element of  $GF(2^8)$ .

The example of identifying an element  $\alpha^9$  of the Galois field  $GF(2^8)$  with an irreducible polynomial  $x^8 + x^4 + x^3 + x^2 + 1$ :

$$\begin{aligned} \alpha^9 &= \alpha \cdot \alpha^8 \\ &= \alpha \cdot (\alpha^4 + \alpha^3 + \alpha^2 + 1) \\ &= (\alpha^5 + \alpha^4 + \alpha^3 + \alpha) \end{aligned}$$

The vector associated with the polynomial  $\alpha^5 + \alpha^4 + \alpha^3 + \alpha$  is calculated as:

$$\begin{array}{cccccccc} \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{array}$$

The elements of  $GF(2^8)$  and the vector associated to each element of the field is tabulated in the Table 1.

Step 2:

The number of proper subfields of  $GF(2^8)$  are:  $q = (\text{Number of positive divisors of } 8) - 1 = 3$ , which are  $F_2, F_{2^2}$  and  $F_{2^4}$ .

Here,  $o(F_2) = 2, o(F_{2^2}) = 4$  and  $o(F_{2^4}) = 16$ .

Let us consider one of the primitive elements of  $GF(2^8)$ ,  $\alpha$  for tracing the elements of the subfields  $F_2, F_{2^2}$  and  $F_{2^4}$ .

$$F_2 = \{0\} \cup \langle \alpha^{\frac{255}{1}} \rangle = \{0, 1\} = \{00000000, 00000001\}$$

$$\begin{aligned} F_{2^2} &= \{0\} \cup \langle \alpha^{\frac{255}{3}} \rangle \\ &= \{0, 1, \alpha^{85}, \alpha^{170}\} \\ &= \{0, 1, \alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha, \alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1\} \\ &= \{00000000, 00000001, 11010110, 11010111\} \end{aligned}$$

$$\begin{aligned}
F_{2^4} &= \{0\} \cup \langle \alpha^{255} \rangle \\
&= \left\{ 0, 1, \alpha^{17}, \alpha^{34}, \alpha^{51}, \alpha^{68}, \alpha^{85}, \alpha^{102}, \alpha^{119}, \alpha^{136}, \right. \\
&\quad \left. \alpha^{153}, \alpha^{170}, \alpha^{187}, \alpha^{204}, \alpha^{221}, \alpha^{238} \right\} \\
&\quad 0, 1, (\alpha^7 + \alpha^4 + \alpha^3), (\alpha^6 + \alpha^3 + \alpha^2 + \alpha), (\alpha^3 + \alpha), \\
&\quad (\alpha^7 + \alpha^4 + \alpha^3 + 1), (\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha), \\
&\quad (\alpha^6 + \alpha^2), (\alpha^7 + \alpha^4 + \alpha + 1), \\
&\quad (\alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1), (\alpha^7 + \alpha^4 + \alpha), \\
&\quad (\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1), \\
&\quad (\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2), \\
&\quad (\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1), \\
&\quad \left. (\alpha^6 + \alpha^2 + 1), (\alpha^3 + \alpha + 1) \right\} \\
&= \left\{ \begin{array}{l} 00000000, 00000001, 10011000, 01001110, 00001010, \\ 10011001, 11010110, 01000100, 10010011, 01001111, \\ 10010010, 11010111, 11011100, 11011101, 01000101, \\ 00001011 \end{array} \right\}
\end{aligned}$$

The distinct elements in all the proper subfields of the chosen Galois field could be identified only by the person who has the knowledge of the chosen Galois field which is private to the system. Thus, an adversary has no knowledge of the input values which ought to be the no. of 0s and 1s in the code words associated with the subfield elements.

**Table 1.** Elements of  $GF(2^8)$

Primitive Element ( $\alpha$ ) Power	Polynomial	Vector
$\alpha^{-inf}$	0	00000000
$\alpha^0$	1	00000001
$\alpha^1$	$\alpha$	00000010
$\alpha^2$	$\alpha^2$	00000100
$\alpha^3$	$\alpha^3$	00001000
$\alpha^4$	$\alpha^4$	00010000
$\alpha^5$	$\alpha^5$	00100000
$\alpha^6$	$\alpha^6$	01000000
$\alpha^7$	$\alpha^7$	10000000
$\alpha^8$	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	00011101
$\alpha^9$	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha$	00111010
$\alpha^{10}$	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$	01110100
$\alpha^{11}$	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3$	11101000
$\alpha^{12}$	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + 1$	11001101
$\alpha^{13}$	$\alpha^7 + \alpha^2 + \alpha + 1$	10000111
$\alpha^{14}$	$\alpha^4 + \alpha + 1$	00010011
$\alpha^{15}$	$\alpha^5 + \alpha^2 + \alpha$	00100110
$\alpha^{16}$	$\alpha^6 + \alpha^3 + \alpha^2$	01001100
$\alpha^{17}$	$\alpha^7 + \alpha^4 + \alpha^3$	10011000
$\alpha^{18}$	$\alpha^5 + \alpha^3 + \alpha^2 + 1$	00101101
$\alpha^{19}$	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha$	01011010
$\alpha^{20}$	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^2$	10110100
$\alpha^{21}$	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	01110101
$\alpha^{22}$	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha$	11101010
$\alpha^{23}$	$\alpha^7 + \alpha^6 + \alpha^3 + 1$	11001001
$\vdots$	$\vdots$	$\vdots$
$\alpha^{254}$	$\alpha^7 + \alpha^3 + \alpha^2 + \alpha$	10001110

Step 3:

Let us define an encoding function  $e: B^8 \rightarrow B^{10}$  by  $e(x_1x_2x_3x_4x_5x_6x_7x_8) = (x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10})$  where  $x_9 = x_1 \oplus x_2 \oplus x_4 \oplus x_6 \oplus x_7$  and  $x_{10} = x_1 \oplus x_3 \oplus x_4 \oplus x_8$ . The parity check matrix is  $P = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ .

Different parity matrices in an encoding function yield different functional values for the same code word, thereby responsible to generate different pass codes.

Step 4:

The elements of the subfields  $F_2, F_{2^2}$  and  $F_{2^4}$  are mapped with the code words of  $B^8 \leftrightarrow B^{10}$  corresponding to the defined encoding function in the step 3 which is depicted in the Table 2.

**Table 2.** Mapping of  $B^8 \leftrightarrow B^{10}$

Subfield	$B^8$	$B^{10}$
$F_2$	00000000	0000000000
	00000001	0000000101
	00000000	0000000000
$F_{2^2}$	00000001	0000000101
	11010110	1101011010
	11010111	1101011111
$F_{2^4}$	00000000	0000000000
	00000001	0000000101
	10011000	1001100000
	01001110	0100111010
	00001010	0000101010
	10011001	1001100101
	11010110	1101011010
	01000100	0100010000
	10010011	1001001111
	01001111	0100111111
	10010010	1001001010
	11010111	1101011111
	11011100	1101110000
11011101	1101110101	
01000101	0100010101	
00001011	0000101111	

Excluding the repeated elements in the subfields, a total of 16 booths are possible in the example whose private keys are listed in the Table 3. Therefore,  $l = 16$ .

**Table 3.** Private key of each booth

Booth	$B^8$	$B^{10}$
1	00000000	0000000000
2	00000001	0000000101
3	11010110	1101011010
4	11010111	1101011111
5	10011000	1001100000
6	01001110	0100111010
7	00001010	0000101010
8	10011001	1001100101
9	01000100	0100010000
10	10010011	1001001111
11	01001111	0100111111
12	10010010	1001001010
13	11011100	1101110000
14	11011101	1101110101
15	01000101	0100010101
16	00001011	0000101111

Step 5:

The voter inputs the voter ID which is sent as an input to the pass code framer. Sequentially, the voter is mapped with one of the booths which are uniquely identified through the mapped code words. The number of voters that could be assigned to a single booth is equal to the number of parity check matrices possible through the proposed encoding function. The input by the voter, the codeword in  $B^8$  which is assigned to the specified booth and its corresponding code word in  $B^{10}$  are fed as an input to the PRKG to compute the required pass code. The Voter ID and the pass code combination are noted by the voter which is used to

authenticate the voter to cast vote. The voters who have generated their pass codes are registered in the respective booths and are considered to be authorized. The process is depicted through the Figure 1. Before voting the voters are

verified at their assigned booths to validate their votes. This is performed by capturing their ID and pass code combination verified as illustrated in the Figure 2.

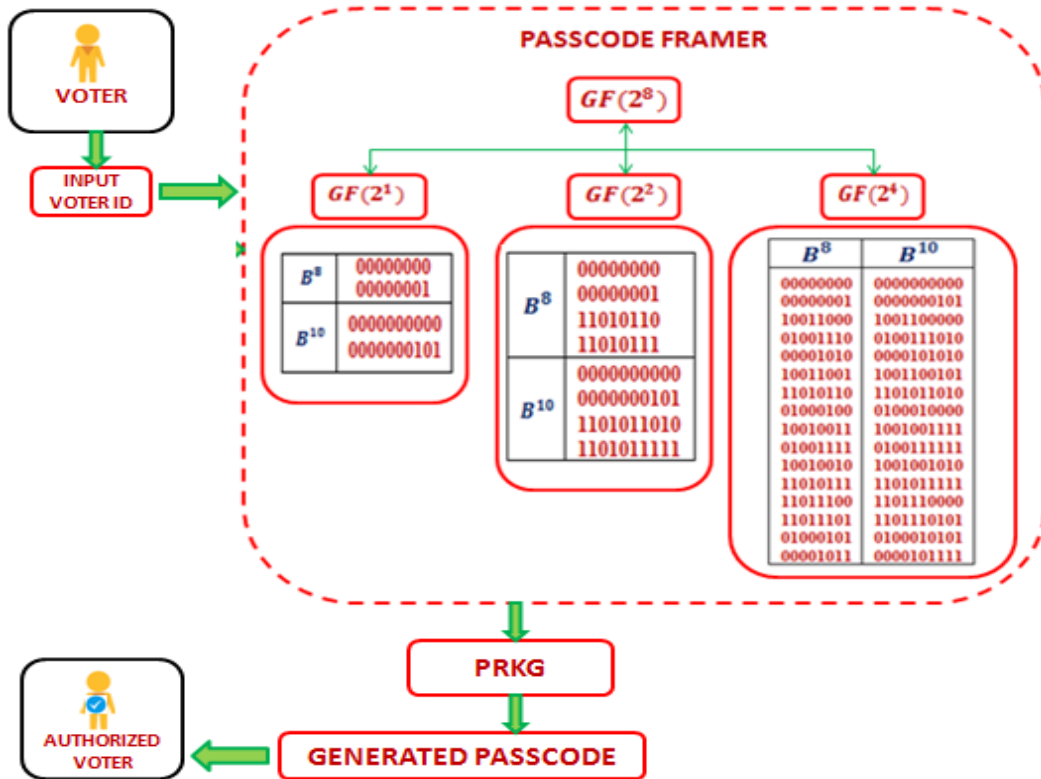


Figure 1. Authorization

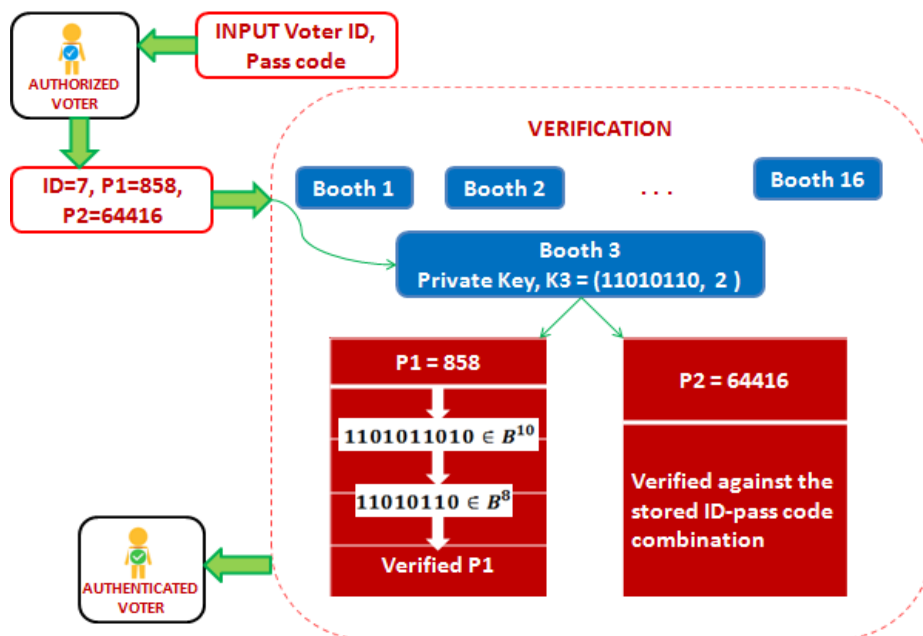


Figure 2. Authentication

The pass code framer generates ID and pass code combination in three segments where the first segment is the ID which determines the assigned booth, the second segment is a decimal equivalent to the code word assigned to the respective booth which determines the correctness of the booth

and the third segment is the pass code generated through the PRKG which is verified against the stored ID-pass code combination. When all the three segments are not a mismatch, the voter is considered to be authenticated and allowed to cast vote.

## 4. ANALYSIS OF THE PROPOSED SCHEME

### 4.1 Security aspects

In authentication schemes, passwords are deduced against unique Ids applying a PRKG. The derived passwords are stored in a vault to verify them against the input Ids to authenticate the user. The other way is to generate a One Time Pad (OTP) which authenticates the user but is valid for a certain instant of time. The OTP generated is also a result of a PRKG. A PRKS is periodic after a certain instant of time and it can be cracked with the knowledge of the input seed. Also, the password-Id combinations are stored in a vault. Hence, the vault needs to be protected from an intruder.

In the proposed scheme, the pass code is generated in two segments where the first part authenticates the booth and the second segment authenticates the pass code against the input voter Id.

Each booth is assigned a private key which is a codeword in  $B^8$ . The assigned codeword is an element of the proper subfields of the Galois Field  $GF(2^8)$ . The first part of the pass code is a decimal equivalent of the codeword in  $B^{10}$  which is the encoding functional value of the private key (codeword in  $B^8$ ) of the booth. An intruder could convert the decimal equivalent to a code word in  $B^{10}$  but to reach the private key one must have the knowledge of the group code  $B^8$  and the encoding function which are private to the system. Hence, the first segment of the pass code is secure.

An intruder can access the data as an authenticated user only when both the segments of the pass code are entered correctly. Although the second part of the pass code is a strong PRKS generated through a PRKG but the input values to the PRKG hail from the first part of the pas code which is resistant to adversarial attacks. The analysis of the applied PRKG is deployed in reference [14]. The PRKG algorithm is implemented using a DEV C++ compiler on an Intel CORE i3 processor with a speed of 1.70GHz and 4.00GB RAM using Windows 8.1 64-bit Operating System. The time taken to generate a single pass code through the PRKG is less than a millisecond which ensures the efficiency of the PRKG.

### 4.2 Applicability of the model in medium scale elections

In the example discussed, with a change in the parity check matrix, different pass codes can be produced with regard to the same element in  $B^8$ . In fact, 212 different parity check matrices can be used for generating different keys with the same combination of  $GF(2^8)$ ,  $B^8$  and  $B^{10}$ . Thus, a single element of the subfield serves as the private key to the booth which could accommodate  $2^{12}$  voters. Since the total number of elements in the subfields of  $B^8$  are 16, therefore the total number of voters with authorization cannot exceed  $2^{12} * 16 = 65,536$ . For the illustration provided above, the contesting of election is feasible for a maximum of 65,536 number of participants. Thus, the developed model is applicable in Internet Voting to organize medium scale elections.

The proposed method can entertain a large scale election by applying encoding function from  $B^8$  to  $B^m$  where  $m > 10$  to increase the number of voters in each booth. Also, with a suitable choice of  $m$  in a Galois field  $GF(2^m)$ , the number of election participants could be increased as the number of subfields depends on the value of  $m$ . With a change in the chosen irreducible polynomial, the same configuration can be used for generating different pass codes for the same election

participants.

## 5. CONCLUSIONS

An efficient and secure pass code generation technique is proposed applying mathematical and cryptographic tools whose application in an OVS is witnessed. PRKG are periodic over a certain instant of time and rely on a predictable input seed value. The developed authentication scheme is advantageous over the systems which apply only Pseudo random numbers generators to authenticate the user. Our method ensures a two-factor authentication by generating the pass code in two segments. The first segment of the pass code is reliable and retains security as long as the encoding function, Galois field and the irreducible polynomial utilized in the method are private to the system. The developed method facilitates authorization and authentication in medium scale elections with a suitable choice of the chosen Galois field  $GF(2^a)$  and the domain  $B^a$  and co-domain  $B^b$ ,  $b > a$  of the encoding function  $e$  and hence satisfies the important criteria of eligibility in an e-Voting scheme. The proposed model is also helpful in telemedicine to provide authorization and authentication to the legitimate parties involved in an e-HCS platform.

## ACKNOWLEDGMENT

This work is supported by GITAM in the form of Dr. M.V.V.S Murthi research fellowship for which we are grateful.

## REFERENCES

- [1] Tomlinson, M., Tjhai, C.J., Ambroze, M.A., Ahmed, M., Jibril, M. (2017). Password correction and confidential information access system. *Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications*, 451-463. [https://doi.org/10.1007/978-3-319-51103-0\\_18](https://doi.org/10.1007/978-3-319-51103-0_18)
- [2] Stinson, D.R., Paterson, M.B. (2019). *Cryptography Theory and Practice* (4th ed.). CRC Press, Taylor & Francis Group.
- [3] Furukawa, J., Mori, K., Sako, K. (2010). An implementation of a mix-net based network voting scheme and its use in a private organization. In *Towards Trustworthy Elections: New Directions in Electronic Voting*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 141-154. [https://doi.org/10.1007/978-3-642-12980-3\\_8](https://doi.org/10.1007/978-3-642-12980-3_8)
- [4] Kho, Y.X., Heng, S.H., Chin, J.J. (2022). A review of cryptographic electronic voting. *Symmetry*, 14(5): 858. <https://doi.org/10.3390/sym14050858>
- [5] Satizábal, C., Páez, R., Forné, J. (2022). Secure internet voting protocol (SIVP): A secure option for electoral processes. *Journal of King Saud University-Computer and Information Sciences*, 34(6): 3647-3660. <https://doi.org/10.1016/j.jksuci.2020.12.016>
- [6] Jayanti, S., Chittibabu, K., Chaganti, P., Sekhar, C. (2023). A novel cryptosystem of an upgraded classical cipher and rsa algorithm for a secure and an efficient electronic voting system. *Journal of Theoretical and Applied Information Technology*, 101(4): 1568-1578.

- <http://www.jatit.org/volumes/Vol101No4/34Vol101No4.pdf>
- [7] Porkodi, C., Sangavai, K. (2021). Matrix based single authority electronic voting schemes. In Proceedings of the First International Conference on Combinatorial and Optimization, ICCAP 2021, Chennai, India. <http://doi.org/10.4108/eai.7-12-2021.2314706>
- [8] Falkner, S., Kieseberg, P., Simos, D.E., Traxler, C., Weippl, E. (2014). E-voting authentication with QR-codes. In Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, Springer International Publishing, 2: 149-159. [https://doi.org/10.1007/978-3-319-07620-1\\_14](https://doi.org/10.1007/978-3-319-07620-1_14)
- [9] Amiruddin, A., Ratna, A.A.P., Sari, R.F. (2019). Construction and analysis of key generation algorithms based on modified Fibonacci and scrambling factors for privacy preservation. *International Journal of Network Security*, 21(2): 250-258. [https://doi.org/10.6633/IJNS.201903\\_21\(2\).09](https://doi.org/10.6633/IJNS.201903_21(2).09)
- [10] Verma, I., Jain, S. (2016). Biometric based key-generation system for multimedia data security. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 864-869. <https://ieeexplore.ieee.org/abstract/document/7724387>.
- [11] Cody Planteen. (2019). Primitive elements and irreducible polynomials of  $GF(256)$ . <https://codyplanteen.com/notes/rs>.
- [12] Lidl, R., Niederreiter, H. (1994). *Introduction to Finite Fields and Their Applications*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139172769>
- [13] Tremblay, J.P., Manohar, R. (1997). *Discrete Mathematical Structures with Applications to Computer Science*. TATA McGraw-Hill Edition.
- [14] Jayanti, S., Chittibabu, K., Akkapeddi, C.S. (2022). Pseudorandom numbers generation: An implementation to a secure cryptosystem. *Neuro Quantology*, 20(9): 944-947. <https://doi.org/10.14704/nq.2022.20.9.NQ440104>