All Sciences Proceedings

1st International Conference on Pioneer and Innovative Studies

June 5-7, 2023 : Konya, Turkey

ICPIS

All Sciences Proceedings
http://as-proceeding.com/



https://as-proceeding.com/index.php/icpis

# A ramp secret sharing scheme from finite fields

Selda Çalkavur*, Patrick Solé [2]

[1]Department of Mathematics/Faculty of Arts and Science, Kocaeli University, Turkey
[2]CNRS, I2M/Centrale Marseille, Aix Marseille University, France

*(selda.calkavur@kocaeli.edu.tr)

***Abstract*** – A ramp secret sharing scheme is a cryptographic method to encode a secret $s$ into multiple shares $s_1, s_2, \dots, s_n$ that only from specified subsets of the shares one can recover $s$. In this paper, we construct a strong ramp secret sharing scheme based on finite fields.

*Keywords – Secret Sharing, Threshold Secret Sharing Scheme, Ramp Secret Sharing Scheme, Finite Fields, Extension Fields*

## I. INTRODUCTION

A secret sharing scheme is a method to encrypt secret information $s$ into $n$ pieces called shares $s_1, s_2, \dots, s_n$ each of which has no information of secret $s$, but $s$ can be decrypted by collecting several shares. For example, consider a $(k, m)$- threshold secret sharing scheme. Any $k$ out of $m$ shares can decrypt secret $s$, but, any $k-1$ or less shares do not leak any information of $s$ in this secret sharing scheme. The original secret sharing scheme [12] and Blakley [1] is a $(k, m)$- threshold secret sharing scheme. It can be explained in two ways. In the case of $(k, m)$- threshold access structure, we assume that every share is equally important, but there are cases such that we want to make some shares more important than the others. Another extension of $(k, m)$- threshold secret sharing schemes is the ramp secret sharing scheme. Ramp secret sharing schemes were proposed independently by Blakley-Meadows [2] and Yamamoto [13], [14] in 1984. A ramp secret sharing scheme is a secret sharing scheme with intermediate properties between qualified and forbidden sets [4]. In a ramp scheme, a secret can be shared among a group of participants in such a way that only sets of at least $k$ participants can reconstruct the secret and $k-1$ participants can not [6].

In this work, we first consider a ramp secret sharing scheme based on finite fields by using representation the elements of finite fields. We characterize the access structure of this scheme, explain its privacy by means of [3], and analyze the security of the scheme.

The rest of the paper is structured as follows. Firstly, a summary of the known some results about finite fields in Section II. Section III gives necessary information about secret sharing schemes. The next section describes the scheme and analyses its security. The last section collects concluding remarks.

## II. ALGEBRAIC PRELIMINARIES

We shall begin with the necessary information to explain our scheme.

### A. *Field Extensions*

Let $F$ be a field. A subset $K$ of $F$ that is itself a field under the operations of $F$. Then, $F$ is called an extension field of $K$. If $K \neq F$, then $K$ is a proper subfield of $F$.

**Definition 1 ([9]).** Let $L$ be an extension field of $K$. If $L$, considered as a vector space over $K$, is finite dimensional, then $L$ is called a finite extension of $K$. The dimension of the vector space $L$ over $K$, it is denoted by symbol $[L: K]$.

### B. *Characterization of Finite Fields*

For every prime $p$ the residue class ring $Z/(p)$ forms a finite field with $p$ elements which may be identified with the Galois field $F_p$ of order $p$. The

fields $F_p$ play an important role in general field theory since every field of characteristic $p$ must contain an isomorphic copy of $F_p$ and can thus be thought of as an extension of $F_p$, This observation, together with the fact that every finite field has prime characteristic is fundamental for the classification of finite fields.

**Lemma 1 ([9]).** Let $F$ be a finite field containing a subfield $K$ with $q$ elements. Then $F$ has $q^m$ elements, where $m = [F:K]$.

**Theorem 1 ([9]).** Let $F$ be a finite field. Then $F$ has $p^n$ elements, where the prime $p$ is the characteristic of $F$ and $n$ is the degree of $F$ over its prime subfield.

**Theorem 2 ([9]). (Subfield Criterion)** Let $F_q$ be the finite field with $q = p^n$ elements. Then every subfield of $F_q$ has order $p^m$, where $m$ is a positive divisor of $n$. Conversely, if $m$ is a positive divisor of $n$, then there is exactly one subfield of $F_q$ with $p^m$ elements.

### C. *Representation of Elements of Finite Fields*

There are different ways of representing the elements of a finite field $F_q$ with $q = p^n$ elements, where $p$ is the characteristic of $F_q$. We examine one of them.

We know that $F_q$ is a simple algebraic extension of $F_p$. In fact, if $f$ is an irreducible polynomial in $F_p[x]$ of degree $n$, then $f$ has a root of $\alpha$ in $F_q$ and so $F_q = F_p(\alpha)$. Therefore, every element of $F_q$ can be uniquely expressed as a polynomial in $\alpha$ over $F_p$ of degree less than $n$.

## III. SECRET SHARING SCHEMES

Secret sharing has been a subject of study for over 30 years. It is important that a secret key, passwords, informations of the map of a secret place, or an important chemical formula, etc. must be kept secret. One of the ways of solving this problem is to employ secret sharing schemes. The main problem for a secret sharing is to divide the secret into pieces instead of storing the whole. A secret sharing scheme is a way of distributing a secret among a finite set of people such that only some distinguished subsets of these subsets is called the access structure of the scheme.

### A. *Ramp Secret Sharing Schemes*

A ramp secret sharing scheme is a cryptographic method to encode a secret $s$ into multiple shares $s_1, s_2, \dots, s_n$ so that only from specified subsets of the shares one can recover $s$. The encoding is in general probabilistic, meaning that to each secret $s$ there corresponds a collection of possible share vectors $s = (s_1, s_2, \dots, s_n)$.

Ramp secret sharing schemes have a trade-off between security and coding efficiency [2], [8], [11], [14]. For example, in the $(k, n, m)$- threshold ramp secret sharing scheme, we can recover $s$ from randomly $k$ or more shares, but no information of $s$ can be obtained from $k - n$ or less shares [2], [7]. Moreover, any $k - l$ shares leak out about $s$ for $l = 1, 2, \dots, n-1$. If $n = 1$, then this $(k, n, m)$-threshold secret sharing scheme means the ordinal $(k, m)$- threshold ramp secret sharing scheme. If a ramp secret sharing scheme does not leak out any part of a secret explicitly from any randomly $k - l$ shares, $l = 1, 2, \dots, n$, then this scheme is called a strong ramp secret sharing scheme [5].

Geil et al. examined the following definition [3]:

A linear ramp secret sharing scheme is said to have $t$- privacy if from no set of size $t$ one can deduce any information about the secret, but from some set of size $t + 1$ can recover some information about it.

## IV. THE SCHEME

In this section, we examine a strong ramp secret sharing scheme based on finite fields.

Consider a finite field $F_q$, where $q = p^n$, $p$ is prime, $n$ is a positive integer. It is clear that $|F_q| = p^n$. We know that every element of $F_q$ can be represented by $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}, a_i \in F_p, i = 0, 1, \dots, n-1,$ and it can be written $p^n$ elements in this way. These elements are also represented as a vector $(s_1, s_2, \dots, s_n)$, $s_j \in F_p$, $j = 1, 2, \dots, n$.

Let the $F_q = F_{p^n} = \{v_1, v_2, \dots, v_{p^n}\}$ be the set of all shares and the secret $s = (s_1, s_2, \dots, s_n)$ be any element of $F_q$. $s$ has into multiple shares $(s_1, s_2, \dots, s_n)$. Suppose that any coordinate of $s$ is known. There are altogether $\frac{p^n}{p} = p^{n-1}$ shares whose any coordinate is nonzero element of $F_q$. So, $p^{n-1} - 1$ out of $p^{n-1}$ shares can recover the secret by combining their shares as follows.

$$x_1 + x_2 + \cdots + x_{p^{n-1}-1} \equiv 0 \ (mod\ p)$$

In this scheme, $n$ must be at least 2. Because if $n = 1$, then we get an ordinal $(k, m)$- threshold

secret sharing scheme. If $(p^{n-1}-1)-l$ say, with $1 \le p^{n-1}-1-l < p^n$ shares group together they can guess the secret with probability

$$\frac{1}{p^{n-1}-l} \le \frac{1}{2}.$$

If $n$ is a small number, in this case the number of shares recovering the secret will be reduced and the worst case for security. So, if $n$ is big enough, then the security will be better.

**Proposition 1.** The finite field $F_{p^n}$ determines a $(p^{n-1}-1, n, p^n)$- ramp secret sharing scheme for $n \in Z^+$ and $p$ is prime.

**Proof.** There are $p^n$ shares since $F_{p^n} = \{v_1, v_2, \dots, v_{p^n}\}$ is the set of all shares and $p^{n-1}$ vectors whose any coordinate is nonzero element of $F_{p^n}$. The secret $s$ multiple shares $(s_1, s_2, \dots, s_n)$. In this scheme, $(p^{n-1}-1)$ out of $(p^n-1)$ shares can recover the secret by using structure of a finite field.

**Corollary 1.** The ramp secret sharing scheme based on finite fields is a strong ramp secret sharing scheme.

**Proof.** In this scheme, it does not leak out any part of a secret explicitly from any arbitrarily $(p^{n-1}-1-l)$ shares for $l = 1, 2, \dots, n$. So, it is also a strong ramp secret sharing scheme.

**Corollary 2.** The ramp secret sharing scheme satisfied the hypothesis of Proposition 1 is said to have $(p^{n-1}-2)$ privacy.

**Proof.** It is clear that $(p^{n-1}-2)+1 = (p^{n-1}-1)$ shares can recover the secret, but $(p^{n-1}-2)$ elements can not.

**Corollary 3.** The number of elements of access structure is $(p^{n-1}-1)$ and the number of total sharing is $(p^{n-1}-1)n$.

**Proof.** Each $s$ has into multiple $n$ shares. There are $(p^{n-1}-1)$ shares recovering the secret in our scheme. So, the number of total sharing is $(p^{n-1}-1)n$. It is seen that $(p^{n-1}-1)$ shares can recover the secret. These shares are also the elements in the access structure.

**Numerical Example 1.** Let $F_{2^4}$ be the secret space. Consider the polynomial $f(x) = x^4 + x + 1$ which is irreducible over $F_2$. Let $\alpha$ be a root of $f$. We know that if $f \in F_2[x]$ is an irreducible polynomial over $F_2$ of degree 4, then by adjoining a root of $f$ to $F_2$, we get a finite field with $2^4$ elements. We also know that each element of $F_2$ can be represented by $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$, $(a_0, a_1, a_2, a_3 \in F_2)$ and it can be written $2^4$ elements in this way. These elements are also represented as a vector $(s_1, s_2, s_3, s_4)$. So,

$$F_{2^4} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$$

and therefore

0=(0000), 1=(1000), $\alpha = (0100)$, $\alpha^2 = (0010)$,
$\alpha^3 = (0001)$, $\alpha^4 = (1100)$, $\alpha^5 = (0110)$,
$\alpha^6 = (0011)$, $\alpha^7 = (1101)$, $\alpha^8 = (1010)$,
$\alpha^9 = (0101)$, $\alpha^{10} = (1110)$, $\alpha^{11} = (0111)$,
$\alpha^{12} = (1111)$, $\alpha^{13} = (1011)$, $\alpha^{14}$=(1001).

Let the secret be , $\alpha^7 = (1101)$. Suppose that the first coordinate is known, that is 1. We also know that there are altogether $p^{n-1} = 2^{4-1} = 8$ vectors whose first coordinate is nonzero. Since one of them is the secret, the remaining 8-1=7 vectors can recover the secret by combining their shares by using the vector addition in the finite field.

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^8 + \alpha^9 + \alpha^{10} + \alpha^{11} + \alpha^{12} + \alpha^{13} + \alpha^{14} + s \equiv 0 \ (mod\ 2)$$

Therefore, it is seen that $s = (1101)$.

If we would knew that the second coordinate is nonzero and chosen such vectors, then we could the secret in this way.

This scheme is also a (7, 4, 16)- ramp secret sharing scheme.

**Numerical Example 2.** Let $F_{3^2} = F_9$ be the secret space. Consider the polynomial $f(x) = x^2 + 1 \in F_3[x]$ which is irreducible over $F_3$. By adjoining a root of $f$ to $F_3$, it is obtained the finite field $F_{3^2} = F_9$ with $3^2 = 9$ elements. Furthermore, each element of $F_{3^2}$ can be represented by $a_0 + a_1\alpha$, $a_0, a_1 \in F_3$ and it can be written 9 elements in this way. These elements are represented as a vector $(s_1, s_2)$. So,

$$F_{3^2} = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha\}$$

and

0=(00), 1=(10), 2=(20), $\alpha = (01), 2\alpha = (02)$,
$1 + \alpha = (11), 2 + \alpha = (21), 1 + 2\alpha = (12)$,
$2 + 2\alpha = (22)$.

Let the secret be $2 + \alpha = (21)$. Assume that the first coordinate is known, that is 2. We also know that there are altogether $p^{n-1} = 3^{2-1} = 3$ vectors whose first coordinate is 2. Since one of them is the secret, remaining 3-1=2 vectors can recover the secret by combining their shares as follows.

$$(20) + (22) + s \equiv 0 \ (mod\ 3)$$
$$s = (12).$$

If we would knew that the second coordinate is 1 and chosen such vectors, then we could reconstructed the secret in this way.

This scheme is a (2, 2, 9)- ramp secret sharing scheme.

### *A. Security Analysis*

We analyze the security of our scheme in this section. It can be examined from the following different views.

1) From the subfield criterion we know that every finite field $F_{p^n}$ has a subfield as $F_{p^m}$, if $m$ is a positive divisor of $n$. But the elements of subfield can not recover the secret. Because the secret $s \in F_{p^n}$ and each secret $s$ into multiple $n$ shares. Hence each element of subfield is length of $m$. This means the elements of subfield have no properties that recovering the secret.
2) In our scheme, $(p^{n-1} - 1)$ out of $(p^n - 1)$ participants can reach the secret but $(p^{n-1} - 2)$ can not. At result, we can say that this ramp secret sharing scheme is very reliable.

## V. CONCLUSION

In the present article, we have constructed a strong ramp secret sharing scheme based on finite fields. Possible attacks have been considered. As a result of this we have said that this scheme is reliable. Moreover, our scheme has the following useful advantages:

1) The shares are elements of a finite field can distribute to participants and then they use the structure of a finite field to recover the secret.
2) Even if the finite field has a subfield, the elements of subfield can not reconstruct the secret since these elements have no properties of the main finite field.

## REFERENCES


[1] G. R. Blakley, *Safeguarding Cryptographic Keys,* in Proc. 1979 National Computer Conf., New York, June, pp. 313-317, 1979.

[2] G. R. Blakley and C. Meadows, *Security of ramp schemes,* Advances in Cryptology-CRYPTO'84, LNCS 196, Springer-Verlag, pp. 242-269, 1985.

[3] O. Geil, S. Martin, U. Martinez-Penas, R. Matsumoto, D. Ruano, *On asymptotically good ramp secret sharing schemes,* Finite Fields and Their Applications, 2015.

[4] M. Iwamoto, *General Construction Methods of Secret Sharing Schemes,* Research Thesis, pp. 1-3, 2003.

[5] M. Iwamoto, H. Yamamoto, *Strongly Secure Ramp Secret Sharing Schemes for General Access Structures,* Information Processing Letters 97, pp. 52-57, 2006.

[6] W-A. Jackson and K. M. Martin, *A Combinatorial Interpretation of Ramp Schemes,* Australasian Journal of Combinatorics 14, pp. 51-60, 1996.

[7] E. G. Karnin, J. W. Greene and M. E. Hellman, *On secret sharing systems,* IEEE Trans. Inform. Theory, vol. 29, no. 1, pp. 35-41, 1983.

[8] K. Kurusawa, K. Okada, K. Sakano, W. Ogata and T. Tsujii, *Nonperfect secret sharing schemes and matroids,* Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-Verlag, pp. 126-141, 1993.

[9] R. Lidl, H. Niederreiter, *Finite Fields,* Encyclopedia of Mathematics and Its Applications, vol. 20, pp. 30-50.

[10] K. Okada and K. Kurusawa, *Lower bound on the size of shares of nonperfect secret sharing schemes,* Advances in Cryptology-ASIACRYPT'94, LNCS 917, Springer Verlag, pp. 34-41, 1994.

[11] W. Ogata and K. Kurusawa, *Lower bound on the size of shares of nonperfect secret sharing schemes,* Journal of Universal Computer Science, vol. 4, no. 8, pp. 690-704, 1998.

[12] A Shamir, *How to share a secret,* Comm. Of the ACM 22 (11), pp. 612-613, 1996.

[13] H. Yamamoto, *Useful codes for secret sharing communication systems,* Technical Reports of IECE, IT84-8:23-29, 1984 (in Japanese).

[14] H. Yamomoto, *On secret sharing systems using $(k, L, n)$- threshold scheme,* IECE Trans., J68-A(9):945-952, 1985 (in Japanese), English translation: Electronics and Communications in Japan, Part I, vol. 69, no. 9, pp. 46-54, Scripto Technica, Inc., 1986.