Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 715–732
DOI : 10.47974/JDMSC-1866

Inside adversary combinatorial attacks in secret sharing scheme via linear system of equations when $n = 5$

L. Sreenivasulu Reddy *
Department of Mathematics
Kalasalingam Academy of Research and Education
Krishnankoil 626126
Tamil Nadu
India

Indrajeet Kumar #
Department of Statistics
Central University of South Bihar
Gaya 824236
Bihar
India

Abstract

When an insider possesses greater than or equal to the threshold number of secret shares, he can retrieve an entire secret without any difficulty. This kind of task doesn't have any big problems. In this work, even if the inside adversary only knows a smaller number of secret shares than the threshold amount, we give the different computational approaches to retrieve the whole secret share. We limit five secret shares in this investigation to be used only for calculation. The assaults in this work are classified into four categories utilising probabilistic and algebraic systems of linear congruence relations, based on the number of secret shares of the adversary and the order of an algebraic field where the secret shares are formed by the distributor. Together with these assaults, this study offers a worst-case and best-case outcome for the inside adversary to retrieve the entire secret. The relationship between the threshold value t and the quantity of secret shares n is the basis of these scenarios. Lastly, we displayed the graphical analysis about the quantity of shares in the secret sharing system as well as the order of an algebraic field in which the distributor creates the secret shares.

Subject Classification: *94A05, 94A60.*

Keywords: *Secret-sharing scheme, Threshold secret sharing scheme, Synchronously, Asynchronously, Hybrid, Perfect secret sharing scheme.*

* *E-mail:* **sreenivasulureddy.svu@gmail.com (Corresponding Author)**
# *E-mail:* **indrajeet.stats@gmail.com**

1. Introduction

Systems for sharing secrets are designed to disperse a secret across a group of confirmed participants so that the combiner–one of the verified participants–can later get the secret. The reason for calling this tactic a "threshold secret sharing scheme" is that the combiner will obtain shares from all authorised participants without really extracting the complete secret. Any threshold secret-sharing technique has two parameters: n and t. In this case, the total number of verified participants is indicated by the parameter n, and the total number of secret shares requested to obtain the whole secret is shown by the parameter t. The threshold secret sharing system with parameters n and t is represented by the (t,n)-threshold secret sharing scheme. Using mathematical principles, the distributor splits the secret into n independent shares such that the later combiner may rebuild the entire secret using any t number of shares. The threshold value of the system is denoted by the parameter t. The threshold secret-sharing strategy is optimal if the whole secret is not retrieved with fewer shares than the threshold number of values secret shares. When all players give their shares to the combiner at the same time during the secret retrieval phase, the process is called synchronous. When participants expose their shares to the combiner one at a time during a covert retrieval method, the process is called asynchronous.

Over the course of three decades, the significance of secret-sharing methods has been seen in a variety of sectors, including cryptography, e-business, network communication, machine learning, etc. All secret-sharing scheme constructions, including (t,n)-threshold schemes, are significantly influenced by a wide range of mathematical ideas, including as field theory, number theory, and numerical techniques. The participant's threshold number of secret shares must be gathered by the combiner via synchronous, asynchronous, or hybrid communication methods in order to produce the complete secret. In secret sharing systems, the impacts of synchronous, asynchronous, and hybrid communication vary in intensity. The kind of communication that takes place in the system's combiner process has not been described in this study. Using a polynomial $f(x) = x^t + \ldots + a_1 x + a_0$ over a finite field F_p, where p is a positive prime integer and $t > 1$ is an integer such that $n \geq t$, many of these (t,n)-threshold secret-sharing systems generate a secret share for authenticated participants. The polynomials play a central role in the field of the threshold secret sharing scheme to create multiple secret shares by the dealer Calkavur et al. [3]. Shamir et al. [19] presented their analysis of the

fourth initial threshold secret-sharing method. Subsequently, Sun, et al. [20] proposed a polynomial-based secret approach; they built their system using the Diffie-Hellman theory. Polynomials were also utilised by Hwang and Chang [9] in the development of their secret-sharing scheme. Ding, et al. [4] recently proposed a safe secret reconstructive secret-sharing technique. Its foundation is asymmetric polynomials and it operates in two variables. Newton's polynomial-based secret-sharing technique was introduced in Bezzateev et al. [2], whereas Çcalkavur et al. [3] suggested a polynomial-based secret-sharing approach that took use of the field extension by degrees structure. Saurabh and Sinha [18] suggested perfect secret-sharing techniques from room squares, a type of combinatorial square, based on specific balanced incomplete block designs that are derived from a larger class of designs known as group divisible designs. Their safe and effective protocol is predicated on a room square of order r, which only occurs when r is odd and $r \neq 3,5$. Using combinatorial techniques, Jackson and Martin [10] suggested the ideal secret-sharing strategies. However, there are certain restrictions associated with secret sharing schemes. These range from the original study conducted by Shamir [19] to the work done by Lemnouar [12], which enumerated the security restrictions associated with the work done by Shamir [19] based on secret sharing scheme. A polynomial interpolation-dependent threshold changeable secret sharing scheme was recently presented by Yuan et al. [22], although Zhang et al. [24] first proposed threshold changeable secret sharing schemes. Mejia and Montoya [14] suggested secret-sharing plans based on information rates homomorphic approaches. To improve security, Mishra and Gupta [15] suggested an iterative secret sharing mechanism with several keys.

Other secret sharing schemes with different designs, such those based on polynomial interpolation, are also implemented in addition to threshold secret sharing methods. For instance, Gharahi and Khazaei [7] investigated the best linear secret-sharing schemes for graph access structures with six participants, and Ersoy, Pedersen, and Anarim [5] looked at homomorphic extensions of CRT-based sharing. Furthermore, Kandar and Dhara [11] examined a verifiable secret-sharing method that included cheater identification and combiner verification. Zhang et al. [23] looked at a reputation-based outsourcing hierarchical threshold secret-sharing method that allows participants at various levels to reconstruct the secret after just one cycle of operation. Qin, Dai, and Wang [17] examined a secret-sharing technique that uses adversarial structure and the (t,n)-threshold to shield participants from their true selves when the

shared secret is changed. Shamir's approach was initially shown by Martin [13] using various forms of cheating in the Lagrange interpolation polynomial-based secret sharing system. They uphold the characteristic of Shamir's scheme, which states that the system's security isn't predicated on any untested theories, such how difficult it is to compute number-theoretic functions. The technique used by Tompa and Woll demonstrates how inside rivals can deceive when shares are disclosed asynchronously. An inside opponent may always release a fake share last under Shamir's asynchronous share distribution technique, ensuring that only the dishonest shareholder can obtain the secret. However, a false secret can also be obtained by other truthful stockholders. Later, Harn, Lin, and Li [8] showed that any secret sharing system may be made vulnerable to manipulation by having an adversary who is an insider reveal their share last during asynchronous sharing. Therefore, Tieng and Nocon [21] first examined the potential for crypt-analysis in Shamir's secret sharing scheme (SSSS) and examined its risks to both a single insider adversary and a group of insider adversaries under synchronous and asynchronous secret sharing when secrets were disclosed synchronously. Abdel and Kim [1] has developed a centralised key generation mechanism based on Shamir's secret sharing method with the assistance of future authentication sensors. picture-based secret sharing approaches using share as a Pixel of the related picture were introduced by Gao, Horng and Chang [6]. In their secret-sharing plan, Ersoy, Pedersen, and Anarim [5] made use of the Chinese remainder theorem and the idea of homomorphism. Using fewer polynomials, Phiri and Kim [16] has presented a linear secret-sharing technique. Ding et al. [4] presented a secret sharing plan in which two variable polynomials, referred to as bivariate polynomials, are used to construct the secret shares.

The current secret-sharing techniques based on polynomials lack adequate information on the following matters: (i) The degree value of the polynomial in a polynomial-based secret sharing scheme has never been disclosed; (ii) The ideal threshold value in a polynomial-based threshold interpolation secret sharing system, such that the system should be flawless and effective. This is the reason we are focusing on insider adversary polynomial-based threshold secret scheme assaults. In this work, we explore that in a polynomial-based threshold secret-sharing scheme, the adversary should be an insider of the system that differs from the combiner. In this study, we take the distributor to be a reliable scheme participant. The scheme's synchronous, asynchronous, or hybrid communication is not specified.

This is how the remainder of the paper is structured. The foundations of polynomial-based secret-sharing systems, such as Shamir's secret-sharing scheme, are briefly reviewed in section 2. The submitted work may be found in sections 3 and 4. In section 3, we outline the best and worst case techniques to obtain a whole secret by inside adversaries, as well as the mathematical justification for selecting threshold values so that the scheme only has one combiner group at a time. In section 4, we outline our primary research effort to calculate the likelihood of obtaining the adversary's complete insider knowledge. We display the graphical result in section 5. In section 6, we finally draw this paper to a close.

2. Preliminaries of polynomial based secret-sharing schemes:

The n authenticated participants in a secret sharing system each have a secret share, represented by the concept s_i for $i = 1,2,3,\ldots,n$. The dealer generates and distributes these shares $s_i s$ by employing a unique function with the input secrets that makes it possible to extract the secrets from the complete set of shares $s_1, s_2, \ldots, s_n$. Occasionally, the secret can be obtained by using an appropriate subset of all the shares. In these cases, the secret-sharing scheme is called a threshold secret-sharing scheme. If no suitable subset of the whole set of shares is able to retrieve the secret, the secret-sharing technique is called perfect. The secret sharing scheme is called a threshold (t,n) -secret sharing scheme if t secret shares out of the entire set of n secret shares are utilised to retry the secret. The threshold approach is ideal if information about t or fewer shares does not disclose any information about the overall secret s. Scholars have offered varying interpretations of Shamir's secret-sharing system; here, we concentrate on the interpretation derived from Lemnouar [12].

Secret sharing schemes are modelled by Shamir's (t,n) threshold secret sharing scheme. This scheme is constructed as a perfect (t,n) threshold system using the numerical process known as Lagrange interpolation. This scheme can be mathematically described as follows: in the field F_p, where a is a non-zero positive integer strictly less than p, the dealer chooses n randomly chosen distinct non-zero values x_i *equivamodp*. Additionally, the polynomial $f(x) = a_0 + a_1 x + \ldots + a_t x^t$ of degree at most t is selected over a field F_p such that the constant term of the polynomial $a_0 \in F_p$ is the secret s other $a_i' s$ for $k = 1,2,...,t$ are constants in the field F_p such that $a_t \equiv 1 \bmod p$. Following that, the distributor computes $y_i = f(x_i)$ for $x_i \equiv a \bmod p)$, where a is any nonzero positive integer strictly smaller than p. The order pairings (x_i, y_i) are then transmitted to a i^{th} participant

who holds the share. Later, the combiner needs at least t shares of (x_i, y_i) to rebuild the equation $f(x) = a_0 + a_1.x + \ldots + a_t x^t$ where $k = t$ such that $a_t \equiv 1 \bmod p$. By employing Lagrande's interpolation polynomial, the combiner is also able to find the secret $s = a_0$.

In any other polynomial-based (t, n)-threshold secret sharing schemes, the combiner of the scheme creates a polynomial using any one of the numerical analysis techniques: Newton's forward, Newton's Backward, Newton's central difference, Lagrane's interpolation, Hermite interpolation and Spline interpolation etc. These methods have their own benefits as well as demerits used in secret sharing schemes. For example, any one of Newton's methods is applied only when the assigned numbers to the authenticated participants are uniform increment in nature. In this work, we consider any type of polynomial construction method.

Assumptions of the secret sharing scheme: In (t, n) threshold secret-sharing systems, the secret distributor and combiner are always reliable parties. The following presumptions underpin the schemes in accordance with these: 1. The distributor is not supposed to be involved in the scam. 2. The nature of the parameters t, n is public. 3. The public nature of each secret share $(x_i, f(x_i))$ is its first component x_i. 4. The secret is a constant term in the polynomial and should be a member of the field F_p. 5. There must be solutions for the system of t non-homogeneous linear equations.

3. Adversaries possibilities on interpolation polynomial based (t, n) -threshold secret sharing schemes:

Our key contribution starts here, discussing the potential adversarial mathematics assaults by an inside adversary employing polynomials in the secret share building process by the distributor, which differs from a combiner on any (t, n) threshold secret-sharing scheme. According to the literature on secret sharing schemes, there isn't a suitable recommendation or evidence for selecting a threshold value of t in the (t, n) threshold secret sharing scheme such that the system is ideal. Perfect in that the opponent cannot obtain all of the secret shares alone if there are fewer than t shares. However, even with flawless current schemes, we find one new issue. The issue is that more than one set of participants may get the complete secret at the same time if t is less than half of the scheme's shares. In this section, we will provide evidence that these types of issues are avoided in all threshold secret-sharing systems with (t, n).

Proposition 3.1: In any (t, n) - threshold secret sharing system, the optimal bound for the threshold parameter t is bigger than $\lfloor n/2 \rfloor$ so long as only one group is integrating the secret at a time.

Proof: Assume that the distributor choose a polynomial of degree $t-1$ such that t is less than or equal to $\lfloor n/2 \rfloor$, where n is the total number of participants who have been authenticated to share the secret in the threshold secret scheme. Afterwards, the combiner gathers t secret shares, including his share, from the n participants in order to rebuild the secret.

As a result, $2t \le n$ since $t \le \lfloor \frac{n}{2} \rfloor$ and $\lfloor \frac{n}{2} \rfloor \le n/2$. As a result, there are more than t different verified participant groups.

Only one group may the combiner be a part of at once.

Therefore, the threshold polynomial may be constructed without the need for a combiner if the other group of t members is able to contribute their secret shares. As a result, $\lfloor n/2 \rfloor$ is bigger than the best bound for the parameter t.

Counter Example :

Assume that the degree of the polynomial is $t = 2$, the public components state $x_i = i$, and there are five authenticated parties in the secret scheme $(n = 5)$. Suppose, then, that of the five twos: The two P_1 and P_3 (one of them a combiner) pool their 8 and 10 shares, respectively. $a(x) = a_0 + a_1 x$ is the polynomial $a(x)$ over the field F_{17}. Compute $a(1)$ and $a(3)$. The two linear equations that result are thus as follows: $a_0 + a_1 = 8$ and $a_0 + 3.a_1 = 10 \in Z_{17}$. In the finite field Z_{17}, there exists a solution for this system such that $a_1 = 1$ and $a_0 = 7$. Thus, $a_0 = 7$ is the secret S. Assume that there is a separate participant group, say P_2 and P_5 (no combiner), that pools its shares, which are 9 and 12, respectively, from the prior participant group. Using the preceding polynomial $a(x) = a_0 + a_1 x$, compute $a(2)$ and $a(5)$. The two linear equations that result are $a_0 + 2.a_1 = 9$ and $a_0 + 5.a_1 = 12 \in Z_{17}$. There is a solution for this system in Z_{17} such that $a_0 = 7$ and $a_1 = 1$. As a result, this set of participants discovers that $a_0 = 7$ is the secret S.

Taking into account this drawback, choose the threshold value t such that the set of authorised participants contains exactly one patrician subset with order t. Thus, only in the case when $t \gtrsim \lfloor n/2 \rfloor$ is this feasible.

Possible assumptions for best and worst case chances of the inside adversary in (t, n) (t, n)-threshold secret sharing schemes.

(i) If the threshold value t of the secret sharing scheme is private, then the inside adversary is not able to find the secret within the time frame and when the scheme has no time frame, there is a chance for the adversary to get the secret with more computation by choosing all possible degree polynomials over the finite field F_p.

(ii) In a scheme, let $x_i's$ be public. If the opponent knows $k \neq 1$ shares of (x_i, y_i), he may compute the secret $S = a_0$.

(iii) Let $x_i's$ in a scheme be private. If the adversary knows $k \neq 1$ shares (x_i, y_i) and at least $t-k$ number of additional $x_i's$ values, he may compute the secret $S = a_0$.

(iv) Only the constant term of the polynomial $f(x)$ contains the secret $S = a_0$, which can be readily obtained provided we are aware of the values of the other t coefficients, $a_1, a_2, \ldots, a_t$.

(v) The internal or external adversary has at most $(p-1)(p-2)\ldots(p-t)$ chances to betray the secret if the field F_p size p is tiny.

We have some incomplete knowledge on selecting polynomial coefficients for threshold secret-sharing schemes based on the aforementioned assumptions. In most research investigations, however, the polynomial is univariate and monic. Below are the worst and best methods that attackers can use to generate threshold secret-sharing polynomials, respectively.

Worst case Algorithm:

(i) Choose the coefficients a_i, $i = 0,1,2,\ldots,t$ of the polynomial $f(x) = a_0 + a_1 x + \ldots + a_t x^t$, where $a_t \not\equiv 0 \bmod p$ in the finite field F_p and $a_0 = s$.

(ii) The constant term a_0 has $(p-1)$ chances because a_0 is the total secret which must be non zero.

(iii) The coefficient a_t must be nonzero because the polynomial has degree t, so a_t is chosen in $(p-1)$ ways.

(iv) For the other $t-1$ coefficients a_i, $i = 1,2,\ldots,t-1$, each one is chosen in p ways.

(v) Thus the polynomial is chosen in $(p-1).p.p\ldots(p-1) = (p-1)^2 p^{t_1}$ ways.

Best case Algorithm:

(i) Choose the coefficients a_i, $i = 0,1,2,\ldots,t$ of the polynomial $f(x) = a_0 + a_1x + \ldots + a_tx^t$ from finite field F_p. But in most of the cases, the polynomials have been chosen such that the coefficients are pairwise distinct.

(ii) The constant term a_0 has $(p-1)$ chances because a_0 be the total secret which must be non zero.

(iii) The coefficient a_t must be nonzero because the polynomial has degree t and choose differently from a_0 and 0, so a_t is chosen in $(p-2)$ ways.

(iv) For the other $t-1$ coefficients a_i, $i = 1,2,\ldots,t-1$, each one is chosen in $(p-3),(p-4),\ldots,(p-(t-3))$ ways respectively.

(v) Thus the polynomial is chosen in $(p-1).(p-2).(p-3)\ldots(p-(t-3))$ ways.

4. Role of Inside Adversary

In contrast to the secret key combiner, the enemy in this part is an insider. It is solely aware of the scheme's share and public information. that the enemy is only aware of the public parameters' scheme and its portion. Consequently, it has a single secret share (x_i, y_i). The potential methods of attack for a secret sharing scheme based on interpolation polynomials are covered in this section. Based mostly on the first element of the secret share–public or private–of the verified parties, these attacks may be broadly classified into two categories. Additionally, based on the information provided to the opponent, each is further classified into four subcategories. We explain how an opponent may use the scheme's existing information to attack the secret-sharing system using the threshold shown below. We can apply similar assaults to any threshold secret sharing method in this way.

This is an example of a threshold secret-sharing scheme: it contains five verified participants $(n = 5)$, a degree of $t = 3$ for the polynomial, and public components that say $x_i = i$ and $1 \le i \le 5$. Assume that the following three participants P_1, P_3, P_5 pool their respective shares, which are 8, 10, and 11, out of the five participants. Since we only have three shares, choose the polynomial $p(x)$ as $p(x) = a_0 + a_1x + a_2x^2$ over the field Z_{17}. $p(1)$, $p(3)$, and $p(5)$ are then computed. The resulting three systems of linear equations in Z_{17} are as follows: $a_0 + a_1 + a_2 = 8$, $a_0 + 3.a_1 + 9.a_2 = 10$, and

$a_0 + 5.a_1 + 8.a_2 = 11$. There is just one solution to this system in Z_{17}, where $a_0 = 13$, $a_1 = 10$, and $a_2 = 2$. Hence, $a_0 = 13$ is the key S.

Case 1: $x_i's$ are public.

First way: Suppose the inside adversary has his secrete share, say (3,10). Here $x_i = i's$ are public and so in each pair , the second component is only a varying quantity. In the field, we have $(p-1) = (17-1) = 16$ number of non-zero elements and among them, one element 10 (the second component of the adversary) is for the adversary. After Adversaryâ€™s second element, the remaining elements are $(p-2) = (17-2) = 15$. Now the adversary has the chance to get the other two pairs of secretes in $(p-3).(p-4) = 14.13 = 182$ ways to get secrete share b_0 such that $b(1) = 8$. Here, the second component of secret share pairs is only varying because they are private.

Second way: Suppose the inside adversary gets one more secret shares of an authenticated participant say $(5,11)$ along with his secret share $(3,10)$. Then it chose a polynomial $b(x) = b_0 + b_1x + b_2x^2$ of degree two such that $b(3) = 10$ and $b(5) = 11$ over the filed Z_{17}, the following two equations are $b_0 + 3b_1 + 9b_2 = 10$ and $b_0 + 5b_1 + 8b_2 = 11$. Eliminate b_3 from both equations and then choosing one value either b_1 or b_2, we get the other. Suppose b_1 is chosen, then we get p number of solutions (b_1, b_2) and among them, remove $b_2 = 0$ because the polynomial degree is two. Thus the total number of possible solutions is $p-1$. Substituting each (b_1, b_2) value in $b_0 + 3b_1 + 9b_2 = 10$ or $b_0 + 5b_1 + 8b_2 = 11$, we get the secret b_0 with $p-1$ possible values. That is there are $p-1 = 17-1 = 16$ chances to find the secret b_0 such that $b(1) = 8$.

Third way: Suppose the inside adversary gets one more secret share of one of the authenticated participants $(5,11)$ along with his secret share $(3,10)$. Then he choose a polynomial $b(x) = b_0 + b_1x + b_2x^2$ of degree two such that $b(3) = 10$ and $b(5) = 11$ over the field Z_17, the following two equations are $b_0 + 3b_1 + 9b_2 = 10$ and $b_0 + 5b_1 + 8b_2 = 11$. Since $x_i = i$'s are public, it can pick any one of $x_i = i$'s other than the above two $x_i = i$'s. For example, he picks $x_1 = 1$ then substitutes in $b(x)$, we get $b(1) = b_0 + b_1 + b_2$ and this value is not known, say $b(1) = a$. Find a such that the system of equations $b_0 + 3b_1 + 9b_2 = 10$, $b_0 + 5b_1 + 8b_2 = 11$, and $b_0 + b_1 + b_2 = a$ has a unique solution such that $a \neq 0, 10, 11$ *modulop*. Because every authenticated party has its own different shares and each has at least some contribution, the value a must be different from other existing share values $10,11$ *modulop* and also non-zero. Thus, there are $p-(k+1)$

$= 17-(2+1) = 14$ possible chances to get $b(1)=8$. Find all $b(x)$ values, so for $x_1=1$ then $b(1)=8$.

Fourth way: Suppose the inside adversary gets secret shares of any one of the authenticated participants, say $(5,11)$ along with his secret share, say $(3,10)$ Then, it chooses a polynomial $b(x)=b_1+b_2.x$ of degree one such that $b(3)=10$ and $b(5)=11$ over the field Z_{17}, the following two equations are $b_1+3b_2=10$ and $b_1+5b_2=11$. Then solving the above equation, we get $b_1=0$ and $b_2=9$ over the field Z_{17}. Thus the polynomial equation $b(x) = b_1+b_2x$ becomes $b(x) = 0+9.x = 9.x$. Since $x_i=i's$ are public, it can take any one of $x_i=i's$ other than the above two $x_i=i's$. For example, it takes $x_1=1$ and then substitutes it in $b(x)$, we get $b(1) = 0+9.1 = 9$ this is the approximate secret value, but the actual secret value is $a_0=13$. The existing secret is near to the original secret, so the adversary can get the exact secret with fewer chances (in the worst case within $(p-2)$ $= 15$. If the degree of the polynomials is greater, then the adversary can get a good approximate value to the secret.

Case 2: $x_i's$ are not public.

First way: Suppose the inside adversary has a secret share, say $(3,10)$. Adversaries need two secret sharing pairs of others because the degree of the polynomial is $t=3$. Here $x_i=i's$ are not public and so in each pair, both the first and second components are varying quantity. In the field, we have $(p-1) = (17-1) = 16$ non-zero elements and so we have $(p-1)$. $(p-1) = 16.16 = 256$ number of order pairs. The secret share order pair $(3,10)$ is known to him, so he needs two other secret sharing order pairs from the remaining $256-1 = 255$ order pairs. He can choose two order pairs among 255 order pairs in $255.(255-1) = 255.254 = 64770$ ways. Thus the adversary has the chance to get the other two pairs of secretes in 64770 ways to get secrete share a_0 such that $a(1)=8$. Here, the second component of secret share pairs is only varying because they are private.

Second way: Suppose the inside adversary has two secret shares including his share, say $(3,10)$ and $(5,11)$. Then he chose a polynomial $b(x) = b_0+b_1x+b_2x^2$ of degree two such that $b(3)=10$ and $b(5)=11$ over the filed Z_{17}, the following two equations are $b_0+3b_1+9b_2 = 10$ and $b_0+5b_1+8b_2 = 11$. Subtracting one equation from the other we get an equation in two variables $b_1,b_2 : 2b_1+16b_2 = 1$. For choosing one value either b_1 or b_2, we get the other. Suppose b_1 is chosen first from F_p, then we get p number of solutions (b_1,b_2) and among them remove $b_2=0$ because the polynomial degree is two. Thus the total number of possible solutions is $p-1$. Substituting each (b_1,b_2) value in $b_0 + 3b_1 + 9b_2 = 10$

or $b_0 + 5b_1 + 8b_2 = 11$, we get the secret b_0 with $p-1$ possible values. That is there are $p-1 = 17-1 = 16$ chances to find the secret b_0 such that $b(3)=10$ and $b(5)=11$. In this way no need to guess others $x_i's$. The computational value is the same as the computational value in the case of $x_i's$ are public.

Third way: Suppose the inside adversary has two secret shares including his share, say (3,10) and (5,11). Then, it can choose a polynomial $b(x) = b_0 + b_1x + b_2x^2$ of degree two such that $b(3)=10$ and $b(5)=11$ over the filed Z_{17}, the following two equations are $b_0 + 3b_1 + 9b_2 = 10$ and $b_0 + 5b_1 + 8b_2 = 11$. Since $x_i = i's$ are not public, it can't pick any exact share with the first component x_i but it can guess in $(p-1)-2 = 14$ ways (other than known shares and zero) from the field F_p, so it has 14 equations. For example, he picks one value from 14 values in the field F_p, says $x_1=1$ then substitutes in $b(x)$, we get $b(1) = b_0+b_1+b_2$ and this value is not known to say $b(1)=a$. Find a such that the system of equations $b_0 + 3b_1 + 9b_2 = 10$, $b_0 + 5b_1 + 8b_2 = 11$, and $b_0 + b_1 + b_2 = a$ has a unique solution such that $a \neq 0, 10, 11$ *modulop*. Because every authenticated party has its own different shares and each has at least some contribution, the value of a must be different from other existing share values 10,11 *modulop* and also non-zero. Thus there are $p-(t+1) = 17-(2+1) = 14$ possible chances to get $b(3)=10$ and $b(5)=11$ Repeat this process for each value from the other 13 values of the field. For each one, we have 14 possible chances to get $b(3)=10$ and $b(5)=11$. Therefore, He finds all $b(x)$ values, so that the secret $a_0=13$ in $14.14=196$ ways.

Fourth way: Suppose the inside adversary has two secret shares including his share, say (3,10) and (5,11). Then, he chose a polynomial $b(x) = b_1+b_2x$ of degree one such that $b(3)=10$ and $b(5)=11$ over the filed Z_{17}, the following two equations are $b_1 + 3b_2 = 10$ and $b_1 + 5b_2 = 11$. Then, solving the above equation, we get $b_1=0$ and $b_2=9$ of x_i over the field Z_{17}. Thus, the polynomial equation $b(x) = b_1 + b_2x$ becomes $b(x) = 0+9.x = 9.x$. Since $x_i = i's$ are not public, he can't pick any one of the exact shares value with the first component x_i, but he can guess the x_i value in $(p-1)-2 = 14$ ways (other than known shares and zero) from the field F_p, so he has 14 equations. For example, he picks one value from 14 values of the filed F_p, says $x_1=1$ then substitutes in $b(x)$, we get $b(1) = 0+9.1 = 9$ this is the approximate secrete value but the actual secret value is $a_0=13$. For every value from the remaining 13 values in the field, repeat these steps. There is just one opportunity for each to obtain $b(3)=10$ and $b(5)=11$. Consequently, it determines the 14 approximation ways for the secret $a_0=13$. Since the current secret is also close to the original secret

in this instance as well, the adversary has a lower probability of obtaining the precise secret (in the worst case, within $(p-2)\,(p-3) = 15.14 = 210$ ways). The opponent can obtain a decent approximation of the secret value if the degree of the polynomials is more than one.

Tabulated Data for these computations.

The consolidated Table 1 for the computational values of outside Adversary on Threshold secret sharing scheme with parameters $(t,n)=(3,5)$.

Table 1

Threshold secret sharing scheme with parameters (*t*, *n*) = (3,5)

Serial No	$x_i's$ are Pubic	$x_i's$ Private	Method
1	$(p-3).(p-4)$	$((p-1)^2-1)$ $((p-1)^2-2)$	Outside Adversary access one secret share value only
2	$p-1$	$p-1$	Outside Adversary access two secret share values only: frame single linear equation from the system of equations.
3	$p-(k+1)$	$p-(t+1)^2$	Outside Adversary access two secret share values only: add one more linear equation to the system of linear equations.
4	$(p-2)$	$(p-2)(p-3)$	Outside Adversary access two secret share values only: choose polynomial of degree two.

5. Graphical Comparison:

This section consists of four graphs each corresponding to the above four types of attacks respectively with the threshold parameter $(t,n)=(3,5)$. These schemes require prime number p such that $p \geq n$. Here we are taking the finite fields $F-p$ of the primes orders respectively {7, 11, 13, 17, 19, 23}.

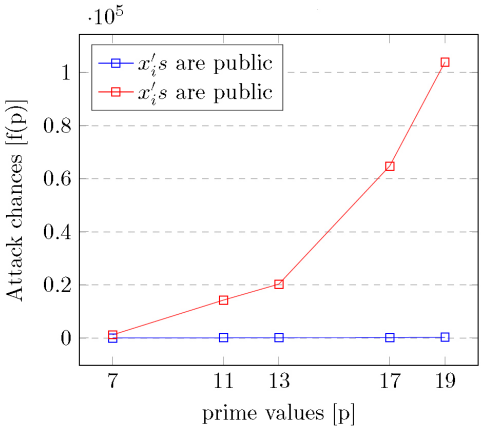

Figure 1

This graph (Figure 1) shows the comparison of possible chances of the inside adversary to get a total secret when he has only his share $(x, f(x))$ information in the manner that the first component is also either private or public.

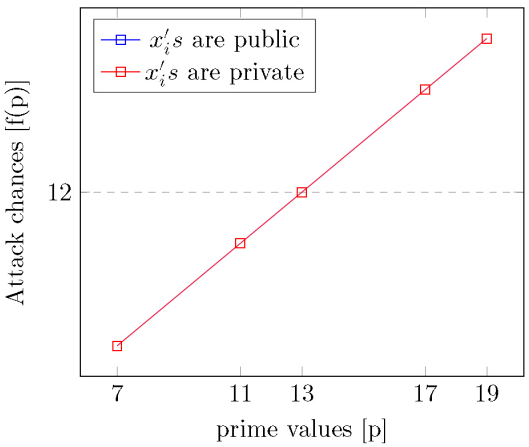

Figure 2

This graph (Figure 2) shows the comparison of possible chances of the inside adversary with a frame of a single linear equation from the system of equations to get a total secret when they have two persons share $(x_1, f(x_1))$ and $(x_2, f(x_2))$ including his share information in the manner that first components are also either private or public.

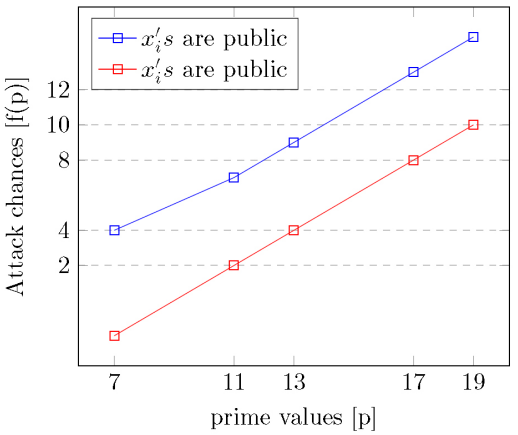

Figure 3

This graph (Figure 3) shows the comparison of possible chances of the inside adversary by adding one more linear equation to the system of linear equations to get a total secret when they know two persons share $(x_1, f(x_1))$ and $(x_2, f(x_2))$ including his share information in the manner that first components are also either private or public.

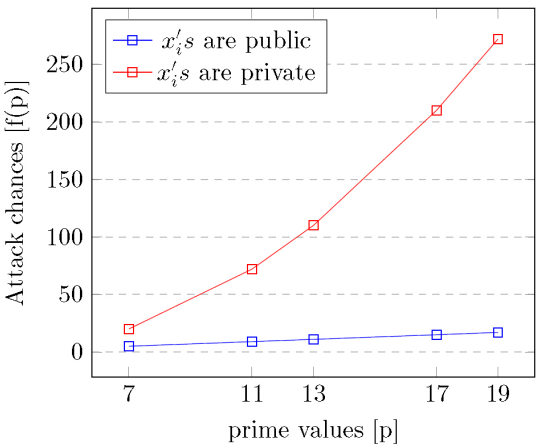

Figure 4

This graph (Figure 4) shows the comparison of possible chances of the inside adversary by choosing a polynomial of degree two to get a total secret when they know two persons share $(x_1, f(x_1))$ and $(x_2, f(x_2))$ including their share information in the manner that first components are also either private or public.

Based on all the data, we can conclude that an attacker will have an easier time figuring out the threshold secret sharing scheme's entire secret if there is more information available to the public.

6. Conclusion

In this study, we see the important contribution of the adversary–an internal scheme participant distinct from the combiner–made by the computational method of identifying particular vulnerabilities in the form of specific computational assaults of the secret sharing schemes. We have researched computational assaults on secret-sharing methods in this regard, particularly threshold secret-sharing techniques. The assaults were split into two categories according to the information sharing components. For the identical problem with five secret shares, four distinct adversary attack methods have been examined and determined to have the same computational numerical value in each case. Furthermore, $t \geq \frac{n}{2}$ is the best constraint for the threshold value t.

In the future, we would want to extend our work by include orders besides the prime and by having a total number of shares n greater than the characteristic of the field. This approach can also be extended to find secrets in threshold secret schemes by considering the combinatorial methods of the inside adversary in a threshold secret sharing scheme and the possible combinatorial methods of the inside/outside adversary in algebraic homomorphism-based threshold secret sharing schemes. The methods may also be applied to threshold bivariate polynomial-based secret-sharing schemes.

Acknowledgments

The authors would like to thank the editor and anonymous reviewers for their positive remarks and useful comments.

References

[1] S. C¸alkavur, P. Sol´ e, and A. Bonnecaze, "A new secret sharing scheme based on polynomials over finite fields," *Mathematics,* vol. 8, no. 8, p. 1200 (2020).

[2] A. Shamir, "How to share a secret," *Communications of the ACM,* vol. 22, no. 11, pp. 612–613 (1979).

[3] H. Sun and S.-P. Shieh, "Construction of dynamic threshold schemes," *Electronics Letters,* vol. 30, no. 24, pp. 2023–2025 (1994).

[4] S.-J. Hwang and C.-C. Chang, "A dynamic secret sharing scheme with cheater detection," in Information Security and Privacy: First Australasian Conference, ACISP'96 Wollongong, NSW, Australia, June 24–26, 1996 Proceedings 1, pp. 48–55, Springer (1996).

[5] J. Ding, P. Ke, C. Lin, and H. Wang, "Bivariate polynomial-based secret sharing schemes with secure secret reconstruction," *Information Sciences*, vol. 593, pp. 398–414 (2022).

[6] S. Bezzateev, V. Davydov, and A. Ometov, "On secret sharing with newton's polynomial for multi-factor authentication," *Cryptography*, vol. 4, no. 4, p. 34 (2020).

[7] S. Saurabh and K. Sinha, "Perfect secret sharing schemes from combinatorial squares," *Security and Privacy,* vol. 5, no. 6, p. e262 (2022).

[8] W.-A. Jackson and K. M. Martin, "Combinatorial models for perfect secret sharing schemes," *Journal of Combinatorial Mathematics and Combinatorial Computing,* vol. 28, pp. 249–266 (1998).

[9] N. Lemnouar, "Security limitations of shamir's secret sharing," *Journal of Discrete Mathematical Sciences and Cryptography*, pp.1–13 (2022).

[10] L. Yuan, M. Li, C. Guo, K.-K. R. Choo, and Y. Ren, "Novel threshold changeable secret sharing schemes based on polynomial interpolation," PloS One, vol. 11, no. 10, p. e0165512 (2016).

[11] Z. Zhang, Y. M. Chee, S. Ling, M. Liu, and H. Wang, "Threshold changeable secret sharing schemes revisited," *Theoretical Computer Science*, vol. 418, pp. 106–115 (2012).

[12] C. Mejia and J. A. Montoya, "On the information rates of homomorphic secret sharing schemes," *Journal of Information and Optimization Sciences*, vol. 39, no. 7, pp. 1463–1482 (2018).

[13] A. Mishra and A. Gupta, "Multi secret sharing scheme using iterative method," *Journal of Information and Optimization Sciences,* vol. 39, no. 3, pp. 631–641 (2018).

[14] M. Gharahi and S. Khazaei, "Optimal linear secret sharing schemes for graph access structures on six participants," *Theoretical Computer Science*, vol. 771, pp. 1–8 (2019).

[15] O. Ersoy, T. B. Pedersen, and E. Anarim, "Homomorphic extensions of crt-based secret sharing," *Discrete Applied Mathematics,* vol. 285, pp. 317–329 (2020).

[16] S. Kandar and B. C. Dhara, "A verifiable secret sharing scheme with combiner verification and cheater identification," *Journal of Information Security and Applications*, vol. 51, p. 102430 (2020).

[17] E. Zhang, J.-Z. Zhu, G.-L. Li, J. Chang, and Y. Li, "Outsourcing hierarchical threshold secret sharing scheme based on reputation," *Security and Communication Networks*, vol. 2019, pp. 1–8 (2019).

[18] H. Qin, Y. Dai, and Z. Wang, "A secret sharing scheme based on (t, n) threshold and adversary structure," *International Journal of Information Security*, vol. 8, no. 5, pp. 379–385 (2009).

[19] K. M. Martin, "Challenging the adversary model in secret sharing schemes," Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts, pp. 45–63 (2008).

[20] L. Harn, C. Lin, and Y. Li, "Fair secret reconstruction in (t, n) secret sharing," *Journal of Information Security and Applications*, vol. 23, pp. 1–7 (2015).

[21] D. G. Tieng and E. Nocon, "Some attacks on Shamir's secret sharing scheme by inside adversaries," Conference Proceedings - The DLSU Research Congress, De La Salle University, Manila, Philippines, Mar. 7-9, pp. 7–9 (2016).

[22] S. A. Abdel Hakeem and H. Kim, "Centralized threshold key generation protocol based on shamir secret sharing and hmac authentication," Sensors, vol. 22, no. 1, p. 331 (2022).

[23] K. Gao, J.-H. Horng, and C.-C. Chang, "An authenticatable (2, 3) secret sharing scheme using meaningful share images based on hybrid fractal matrix," *IEEE access,* vol. 9, pp. 50112–50125 (2021).

[24] K. K. Phiri and H. Kim, "Linear secret sharing scheme with reduced number of polynomials," *Security and Communication Networks,* vol. 2019 (2019).

Received May, 2023