Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 4, pp. 977–989
DOI : 10.1080/09720529.2021.1961902

Security limitations of Shamir's secret sharing

Noui Lemnouar
Department of Mathematics
Faculty of Mathematics and Computer Science
University of Batna2
Batna 05000
Algeria

and

Lamie Laboratory
University of Batna2
Batna 05000
Algeria

Abstract

The security is so *important* for both storing and transmitting the digital data, the choice of parameters is critical for a security system, that is, a weak parameter will make the scheme very vulnerable to attacks, for example the use of supersingular curves or anomalous curves leads to weaknesses in elliptic curve cryptosystems, for RSA cryptosystem there are some attacks for low public exponent or small private exponent. In certain circumstances the secret sharing scheme is required to decentralize the risk. In the context of the security of secret sharing schemes, it is known that for the scheme of Shamir, an unqualified set of shares cannot leak any information about the secret. This paper aims to show that the well-known Shamir's secret sharing is not always perfect and that the uniform randomization before sharing is insufficient to obtain a secure scheme. The second purpose of this paper is to give an explicit construction of weak polynomials for which the Shamir's (k, n) threshold scheme is insecure in the sense that there exist a fewer than k shares which can reconstruct the secret. Particular attention is given to the scheme whose threshold is less than or equal to 6. It also showed that for certain threshold k, the secret can be calculated by a pair of shares with the probability of 1/2. Finally, in order to address the mentioned vulnerabilities, several classes of polynomials should be avoided.

Subject Classification: *94A60, 94A62, 11T71.*

Keywords: *Elliptic curve, Perfect scheme, RSA cryptosystem, Secret, Shamir's secret sharing, Threshold.*

E-mail: `l.noui@univ-batna2.dz`

© Taru Publications

1. Introduction

Information security is very important for most companies or organizations, it protects sensitive data from the malicious purpose. There are many types of security, elliptic curves and secret sharing schemes are tools required in several cryptographic protocols.

Supersingular curves and anomalous curves are the special classes of elliptic curves that are known to be weak, [1], [2], [3] for discrete logarithm problem, these curves may thus lead to easier attacks (MOV attack, Araki-Semaev-Smart-Satoh attacks).

There are also some attacks on RSA cryptosystem during the last decade [4].

A secret sharing scheme (SSS) is a technique in which a dealer securely distributes shares of a secret S to n participants $P_1,...,P_n$ such that the reconstruction of the information S can be done only by authorized subsets of participants.

Some secret sharing schemes are based on some physical properties, for example the visual secret sharing, [5], [6], and quantum secret sharing schemes, [7], while other schemes used coding theory [8], [9].

The secret sharing scheme has applications in various areas such as multiparty computations, access control, key management and electronic voting.

SSS is initiated in 1979 by Shamir and Blakley [10, 11]. The two authors have used Lagrange interpolation and projective geometry respectively.

Let k, n be positive integers with $k \le n$. (k, n) threshold secret sharing is a special type of SSS where among a group of n participants, any k or more participants can recover the secret while no group of $k-1$ or fewer can do so.

Shamir's (k, n) threshold scheme

Let $K = F_p$ be a finite field of order prime p with $n \le p-1$, let $P = \{P_1, \ldots, P_n\}$ denote the set of participants.

Share distribution

To share a secret $S \in K$, the dealer takes a random polynomial $R(x) = a_{k-1}x^{k-1} + \ldots + a_1 x$ with $a_i \in K$ and forms the polynomial

$$f(x) = a_{k-1}x^{k-1} + \ldots + a_1 x + S$$

and secretly gives the shares $S_i = f(x_i)$ to participant P_i where $x_i \in K - \{0\},\ 1 \le i \le n,$ is a public index associated to P_i.

Share reconstruction phase

k participants or more can calculate the secret S, for example, by using the Lagrange interpolation, indeed, let $\{P_{i1},...,P_{ik}\}k$ participants with their respective shares $S_{i1},...,S_{ik},$ they put $g(x) = \sum_{j=1}^{k} S_{ij}.l_j$ with $l_j = \prod_{r \ne j} \frac{x - x_{ir}}{x_{ij} - x_{ir}}$ and compute $g(0) = S.$

The purpose of our paper is twofold, first, we will show that Shamir's secret sharing is not always perfect and that the uniform randomization before sharing is not sufficient to obtain a secure system, second, to be precise, we introduce the counterpart share and we exhibit classes of polynomials for which the secret can be recovered by a pair of share and its counterpart.

II. Contributions

Let's recall some definitions and results:

- Two integers *a* and *b* are coprime if *their greatest common divisor is*1.
- The Euler phi function

  $\phi(n)$ is the number of integers less than n that are coprime to n.

  Using the prime factorization $n = p_1^{\alpha_1} ... p_m^{\alpha_m}$, [12], $\phi(n)$ can be expressed by

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_m}\right)$$

- The multiplicative group $\left(\left(\frac{Z}{pZ}\right)^*, .\right)$ is cyclic of order $p-1,$ any generator *a* of this group is called primitive root mod *p*, the number of primitive roots mod *p* is $\phi(p-1),$ [12].
- The *Legendre symbol* of an integer *a* modulo an odd prime *p* is 0 if *a* is multiple of *p*, and otherwise + 1 if *a* quadratic residue modulo *p*, and – 1 if not.
- The Legendre symbol is denoted by $\left(\frac{a}{p}\right)$.

So $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ and $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$, [13].

- We introduce the following definition:
  Let p be an odd prime and $a, b \in \left(\frac{Z}{pZ}\right)^*$, b is the *counterpart* (opposite) of a if $a + b = p$.
  The share S_{p-a} is called the counterpart of the share S_a.

In some scenarios, secret sharing schemes with small threshold have more practical significance. Let's start with the case:

2.1 *Threshold k = 2.*

For Shamir 's $(2, n)$ secret sharing scheme, $f(x) = a_1 x + S$. Then for every $x_1 \in F_p - \{0\}$, $f(x_1) + f(p - x_1) = 2S$. In this case the secret can be recovered by every pair of participant P_{x_1} and its counterpart P_{p-x_1} :

$$S = \frac{1}{2}(f(x_1) + f(p - x_1)).$$

2.2 *Threshold k = 3*

For Shamir's $(3, n)$ secret sharing scheme, $f(x) = a_2 x^2 + a_1 x + S$ with $a_2 \in F_p - \{0\}$, then for every $x_1 \in F_p - \{0\}$, $f(x_1) + f(p - x_1) = 2S + 2a_2 x_1^2$.

As $x_1, a_2 \in F_p - \{0\}$, the secret cannot be computed by a pair of share and its counterpart.

In addition to case $k = 4$ presented at conference ICCTIM 2020, [14], we tackle the general case $k = 2m$.

2.3 *Threshold k = 4*

Consider the set $\Im_4^p = \{R(x) = a_1 x + a_3 x^3 \,/\, a_3 \in F_p - \{0\},\ a_1 \in F_p\}$.

If $f \in F_p[x]$ of degree 3, $f(x) = S + b_1 x + b_2 x^2 + b_3 x^3$ is used for Shamir's $(4, n)$ threshold scheme, for every $x_1 \in K - \{0\}$, $f(x_1) + f(p - x_1) = 2S + 2b_2 x_1^2$, then for $b_2 = 0$, the secret S equals the arithmetic mean of two shares S_{x_1} and its counterpart S_{p-x_1}. Hence for every $R(x)$ in $\Im_4^p$ the secret S can be recovered by each of $\frac{p-1}{2}$ specific pairs of participant and its counterpart (P_{x_1}, P_{p-x_1}) where $x_1 \in F_p - \{0\}$.

Example 1 : Let $p = 11$, $R(x) = x^3 + 2x \in \Im_4^{11}$.

Table 1
Computation of shares

x_i	1	2	3	4	5	6	7	8	9	10
S_i	0	9	8	3	0	5	2	8	7	5

Share distribution

Take the secret $S = 8$, then $f(x) = x^3 + 2x + 8,$ the shares are computed in table 1.

Share reconstruction phase

a) By using the Lagrange interpolation, Compute the secret S from the four shares $S_1 = 0, \quad S_2 = 9, \quad S_3 = 8, \quad S_4 = 3.$

Put

$$l_1 = \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)}, \quad l_2 = \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)},$$

$$l_3 = \frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)}, \quad l_4 = \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}$$

So $S = 0 \times l_1(0) + 9 \times l_2(0) + 8 \times l_3(0) + 3 \times l_4(0) = 8.$

b) The secret S can also be obtained by the pairs (S_i, S_{11-i}), $1 \le i \le 5$:

$$S = \frac{0+5}{2} = \frac{9+7}{2} = \frac{8+8}{2} = \frac{3+2}{2} = \frac{0+5}{2} = 8.$$

For threshold $k = 4$, there are $p^3 - p^2$ polynomials $a_1 x + a_2 x^2 + a_3 x^3$ with $a_3 \neq 0,$ among these polynomials there are $\left|\Im_4^p\right| = p^2 - p$ insecure polynomials.

2.4 *Threshold k = 2m*

In the general case $k = 2m, \quad m \ge 2,$ consider

$$\Im_{2m}^p = \left\{ R(x) = \sum_{i=1}^{m} b_i x^{2i-1} \,/\, b_1, ..., b_m \text{ are chosen randomly in } F_p \text{ with } b_m \in F_p - \{0\} \right\}$$

All polynomials of $\Im_{2m}^p$ are weak because for any polynomial $f(x) = S + \sum_{i=1}^{m} b_i x^{2i-1},$ the secret S can be recovered by two specific shares $f(x_1), f(p - x_1)$ where $x_1 \in F_p - \{0\}$:

$$S = \frac{1}{2}(S_{x_1} + S_{p-x_1}).$$

2.5 *Threshold k = 5.*

Consider the set $\Im_5^p = \{R(x) = a_1x - (x_1^2)a_4x^2 + a_3x^3 + a_4x^4 / a_4, x_1 \in F_p - P0\{, a_1, a_3 \in F_p\}$, indeed, if $f \in F_p[x]$ of degree 4, $f(x) = S + b_1x + b_2x^2 + b_3x^3 + b_4x^4$ is used for Shamir's $(5, n)$ threshold scheme, let $x_1 \in K - \{0\}$, then $f(x_1) + f(p - x_1) = 2b_4x_1^4 + 2b_2x_1^2 + 2S = 2S$ if $b_2 = -x_1^2 . b_4$.

In this case the secret S can be calculated by using the two shares $f(x_1)$ and its counterpart $f(p - x_1)$ and all polynomials of $\Im_5^p$ are weak.

- Now we will prove that, for threshold $k = 5$, roughly half of all polynomials of degree 4 are not secure.

Put $Ins_5 = \left|\Im_5^p\right|$, so $Ins_5 = (p-1)\left(\frac{p-1}{2}\right)p^2 = \frac{1}{2}(p-1)^2p^2$, let T_5 denote the number of all polynomials of degree 4, $b_1x + b_2x^2 + b_3x^3 + b_4x^4$ with $b_4 \in F_p - \{0\}$ and $b_1, b_2, b_3 \in F_p$, then $T_5 = (p-1)p^3$.

Compute $\alpha_5(p) = \frac{Ins_5}{T_5} = \frac{1}{2}\left(\frac{p-1}{p}\right)$, when p takes large values, the value of $\alpha_5(p)$ approaches $\frac{1}{2}$.

Example 2 : In the table 2, the value of $\alpha_5(p)$ is calculated for some primes p

- We will prove the previous result by another method: Any polynomial of degree 4, $b_1x + b_2x^2 + b_3x^3 + b_4x^4$ is insecure if $b_2 = -x_1^2 . b_4$, or equivalently, $(-b_2).b_4^{-1} \in K_*^{\,2}$, but for every finite field $K = Z_p$, $\left(\frac{K_*}{K_*^{\,2}}, \bullet\right) \approx \left(\frac{Z}{2Z}, +\right)$. Hence the probability that a random chosen degree-4-polynomial is insecure, equals $\frac{1}{2}$.

2.6 *Threshold k = 6.*

Let the set $\Im_6^p = \{R(x) = a_1x - (x_1^2)a_4x^2 + a_3x^3 + a_4x^4 + a_5x^5 / a_5, x_1 \in F_p - \{0\}, a_1, a_3, a_4 \in F_p\}$

Indeed, if $f \in F_p[x]$ of degree 5, $f(x) = S + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5$ is used for Shamir's $(6, n)$ threshold scheme, let $x_1 \in K - \{0\}$, then $f(x_1) + f(p - x_1) = 2b_4x_1^4 + 2b_2x_1^2 + 2S = 2S$ if $b_2 = -x_1^2 . b_4$.

Table 2

Calculation of $\alpha_5(p)$ for some primes p

p	11	19	29	31	101
$\alpha_5(p)$	0.454	0.473	0.482	0.483	0.495

- If $b_4 = 0$ then $b_2 = 0$ and $f(x) = S + b_1x + b_3x^3 + b_5x^5$, according to 2.4, for every element x_1 in $F_p - \{0\}$ the secret S can be recovered by two shares $f(x_1)$, $f(p - x_1)$.
- If $b_4 \neq 0$ then $b_2 \neq 0$ and the secret S can be computed by $S = \frac{1}{2}(f(x_1) + f(p - x_1))$. Hence all polynomials of $\Im_6^p$ are insecure, put $Ins_6 = \left|\Im_6^p\right|$, so $Ins_6 = (p-1)(p-1)\left(\frac{p-1}{2}\right)p^2 + (p-1)\ p^2 = (p-1)p^2\left[\frac{1}{2}(p-1)^2+1\right]$

  Let T_6 denote the number of all polynomials of degree 5, $b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5$ with $b_5 \in F_p - \{0\}$ and $b_1, b_2, b_3, b_4 \in F_p$, then $T_6 = (p-1)p^4$. Calculate $\alpha_6(p) = \frac{Ins_6}{T_6} = \frac{\frac{1}{2}(p-1)^2+1}{p^2}$, when p gets larger, $\alpha_6(p)$ *tends towards* $\frac{1}{2}$, that is, for threshold $k = 6$, roughly half of all polynomials of degree 5 are insecure.

Example 3 : In the table 3, the value of $\alpha_6(p)$ is calculated for some primes p.

Now by another way we will calculate the probability to obtain an insecure polynomial.

Indeed, we have

$f(x) = S + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5$ is insecure $\Leftrightarrow$ $b_2 = -x_1^2 . b_4$

For $b_4 = 0$, according to 2.4 the polynomial $f(x)$ is insecure.

For $b_4 \neq 0$, using the multiplicative property of Legender symbol [13]:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

We have $f(x)$ is insecure $\Leftrightarrow$ $-b_2$, b_4 are either both square or both non-square.

As half of the numbers in $F_p - \{0\}$ are squares, the probability p_6 of obtaining insecure polynomials can be formulated as follows:

Table 3

Calculation of $\alpha_6(p)$ for some primes p

p	11	19	29	31	101
$\alpha_6(p)$	0.421	0.451	0.467	0.469	0.490

A box $(F_p - \{0\})$ contains $m = \frac{1}{2}(p-1)$ white balls (squares) as well as m black balls (non-squares), two balls are drawn at random, what is the probability p_6 of getting 2 balls of the same color ?

If the two balls are drawn without replacement,

$$p_6 = \frac{\binom{m}{2} + \binom{m}{2}}{\binom{2m}{2}} = \frac{m-1}{2m-1}$$

If the two balls are drawn with replacement,

$$p_6 = \frac{m^2 + m^2}{(m+m)^2} = \frac{1}{2}$$

In all cases an insecure polynomial is obtained with the probability of 1/2.

Remark 1 : *To remedy* the security *weaknesses* of the schemes in 2.5 and 2.6, the trusted dealer must choose the random sequence (b_i) such that only one of the two numbers $-b_2, b_4$ is square.

The following table summarizes the weak polynomials for the threshold k less than or equal to 6

Table 4

Explicit description of weak polynomials $\sum_{i=1}^{k-1} b_i x^i$ for the threshold k less than or equal to 6

Threshold k	Conditions on coefficients b_i	Pairs of shares recovering the secret S
$k = 2$		$\forall x_1 \in F_p^*, S = \frac{1}{2}(S_{x_1} + S_{p-x_1})$
$k = 3$		There are no pairs recovering the secret

Contd...

$k=4$	$b_2=0$	$\forall x_1 \in F_p^*, S=\frac{1}{2}(S_{x_1}+S_{p-x_1})$
$k=5$	$b_2 \neq 0$ and $-b_2$, b_4 are either both square or both non-square.	$\exists x_1 \in F_p^*, S=\frac{1}{2}(S_{x_1}+S_{p-x_1})$
$k=6$	$b_2 \neq 0, b_4 \neq 0$ and $-b_2$, b_4 are either both square or both non-square.	$\exists x_1 \in F_p^*, S=\frac{1}{2}(S_{x_1}+S_{p-x_1})$
	$b_2=b_4=0$	$\forall x_1 \in F_p^*, S=\frac{1}{2}(S_{x_1}+S_{p-x_1})$

2.7 *Number generators and Shamir's Secret Sharing*

It is known that in a perfect secret sharing scheme any unqualified subset of participants can learn nothing about the secret, in particular no single share can leak any information about S [15] , in this section, using pseudo-random number generator and a random number generator, we construct a family of polynomials for which the associated Shamir's scheme is insecure.

Case 1. **Pseudo-random number generator (PRNG).**

Pseudo-random generator utilizes computational algorithms to generate numbers.

For this case, we choose Linear congruential generator (LCG) which is one of the oldest and best known pseudorandom generator algorithm, [16]. It is defined by a recurrence relation:

$$X_{i+1} = a.X_i + c \mod m$$

Its parameters are, m the modulus, a the multiplier, c the increment and X_0 the seed.

Let's start by the following example:

Example 4 :

(a) Take $m=p=7$, $a=3$, $c=0$. If the seed X_0 equals 5 we obtain the first $p-2=5$ terms, $X_0=5$, $X_1=1$, $X_2=3$, $X_3=2$, $X_4=6$ and we form the polynomial for Shamir's (6, 6) threshold scheme, $f(x)=5x^5+x^4+3x^3+2x^2+6x+S$

In this scheme, for every secret S, the secret is computed by a single share $f(1) = f(6) = 3 + S$.

b) Generally let $X_0, X_1, ..., X_i ...$ be a sequence generated by a LCG with the relation

$$X_{i+1} = a.X_i \bmod p.$$

This sequence has the longest period $p-1$ if and only if a is a root primitive of p [17].

There are $\varphi(p-1)$ such elements a, in this case, we obtain $p-1$ distinct coefficients $X_0, aX_0, a^2X_0, ..., a^{p-2}X_0$

Let n be the number of participants.

As $n \le p-1$, by using the first $p-2$ terms we form the polynomial $f(x) = X_0.x^{p-2} + aX_0.x^{p-3} + a^2X_0.x^{p-4} + ... + a^{p-3}X_0.x + S$ for Shamir's $(p-1, p-1)$ threshold scheme, then we obtain $f(1) = f(p-1) = S - \frac{X_0}{a}$.

The secure scheme must provide privacy of the secret and shares, but in the obtained scheme the participant P_1 knows the value of its counterpart P_{p-1}. On the other hand, if the dealer uses the same polynomial twice (keeping the same value of $\frac{X_0}{a}$), the participant P_1 can deduce the second secret S_2 from the first S_1: Indeed, if we let s_1' and s_1'' denote respectively the shares of P_1 in the first and the second sharing , then

$$s_1' = S_1 - \frac{X_0}{a},\ s_1'' = S_2 - \frac{X_0}{a} \text{ imply } S_2 = (S_1 - s_1') + s_1''.$$

Case 2. Random number generator (TRNG)

The randomness comes from atmospheric phenomena is better than the pseudo-random generator. To generate numbers TRNG uses some sources of randomness in the physical system like radioactive decay, atmospheric noise, quantum measurements, lasers,...[18]

In this case we choose a generator using true randomness via atmospheric noise, as $n \le p-1$, for example we can use the free services of Random Org /sequences/[19], with 1 the smallest value and $p - 2$ as the largest value. Using the obtained coefficients we form the polynomial of Shamir's $(p-1, p-1)$ threshold scheme, we affirm that all such schemes are insecure because the value of each term occurs once in the

sequence and the secret can be revealed by a single share $f(1)$, because $f(1) = \frac{1+(p-2)}{2}(p-2) + S = 1 + S.$

Then $S = f(1) - 1.$

The permutations of the $p-2$ coefficients give $(p-2)!$ other weak polynomials.

Example 5 : For p =11, Random org gives the sequence

6, 5, 3, 1, 2, 7, 8, 4, 9.

The associated polynomial of Shamir's (10, 10) threshold scheme is $f(x) = 6x^9 + 5x^8 + 3x^7 + x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 9x + S,$ then $S = f(1) - 1.$

Remark 2 : According to [20] , anomalous curves over F_p are elliptic curves $E(F_p)$ whose order is p, they are known to be weak. It follows from [21] that supersingular curves over F_p are elliptic curves $E(F_p)$ whose order is $p+1,$ they are also weak; By analogy, we showed that Shamir's schemes over F_p that are mentioned in the previous subsection, whose threshold is $p-1,$ are weak.

From the previous results, it then follows the following:

a) Shamir's secret sharing is not always perfect and the uniform randomization before sharing is insufficient to obtain a secure scheme.

b) For threshold k = 5 or 6, the secret can be calculated by a pair of shares with the probability of ½.

In conclusion, to increase the security of Shamir's (k, n) -threshold Scheme, on the random sequence one must impose additional conditions on the coefficients $(b_i),$ for example when threshold equals 5 or 6 the trusted dealer must choose the random sequence (b_i) such that only one of the two numbers $-b_2, b_4$ is square.

To eliminate the weaknesses mentioned above, several classes of polynomials should be avoided.

For the threshold k less than or equal to 6, the weak polynomials $\sum_{i=1}^{k-1} b_i x^i$ are described in Table 4.

References

[1] Menezes, A. J., Okamoto, T., & Vanstone, S. A. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. *iEEE Transactions on information Theory*, *39*(5), 1639-1646. DOI: 10.1109/18.259647

[2] Wiener, M. J., & Zuccherato, R. J. (1998, August). Faster attacks on elliptic curve cryptosystems. In *International workshop on selected areas in cryptography* (pp. 190-200). Springer, Berlin, Heidelberg.

https://doi.org/10.1007/3-540-48892-8_15

[3] Abderrahmane Nitaj & Emmanuel Fouotsa (2019) A new attack on RSA and Demytko's elliptic curve cryptosystem, Journal of Discrete Mathematical Sciences and Cryptography, 22:3, 391-409, DOI: 10.1080/09720529.2019.1587827.

[4] Majid Mumtaz & Luo Ping (2019) Forty years of attacks on the RSA cryptosystem: A brief survey, Journal of Discrete Mathematical Sciences and Cryptography, 22:1, 9-29, DOI: 10.1080/09720529.2018.1564201

[5] Abhishek Mishra & Ashutosh Gupta (2018) Multi secret sharing scheme using iterative method, Journal of Information and Optimization Sciences, 39:3, 631-641, DOI: 10.1080/02522667.2017.1385161

[6] Naor, M., & Shamir, A. (1995).Visual Cryptography, Proceedings of the Advances in Cryptology- Eurocrypt'94 (Vol. 950,pp. 1-12). Lecture Notes in Computer Science. ISBN 3-540-60176-7

[7] Deng,F.G., &Long, G.L., & Zhou, H.Y. (2005). An efficient quantum secret sharing scheme with Einstein–Podolsky–Rosen pairs. Physics Letters A, 340, 43-50. https://doi.org/10.1016/j.physleta.2005.04.007

[8] Kim, J.L., & Nari, L. (2017) .Secret sharing schemes based on additive codes over GF (4). Applicable Algebra in Engineering, Communication and Computing, 28(1), 79-97.

DOI 10.1007/s00200-016-0296-5

[9] Sassia, M., & Noui, L. (2019) Characterization of some minimal codes for secret sharing. Asian-European Journal of Mathematics, 12(02), 1950026. https://doi.org/10.1142/S1793557119500268

[10] Shamir, A. (1979) .How to share a secret. Communications of the ACM, 22(11). 612-613. https://doi.org/10.1145/359168.359176

[11] Blakley, G. R. (1979, December). Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on* (pp. 313-313). IEEE Computer Society. DOI: 10.1109/AFIPS.1979.98

[12] Sándor, J., Mitrinovic, D. S., & Crstici, B. (2005). *Handbook of number theory I*. Springer Science & Business Media.
https://doi.org/10.1007/1-4020-3658-2_1.

[13] Kaliski B. (2011) Legendre Symbol. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_418.

[14] Noui Lemnouar (2020) , Weaknesses of Shamir's secret sharing scheme, *International Conference on Computational Techniques and Intelligent Machine,* ICCTIM 2020, Baba Farid College, Bathinda, India, November 26-28, 2020.
https://babafaridgroup.edu.in/ICCTIM-2020/.

[15] C. Lin, L. Harn and D. Ye, "Ideal Perfect Multilevel Threshold Secret Sharing Scheme," *2009 Fifth International Conference on Information Assurance and Security*, Xi'an, 2009, pp. 118-121, doi; 10.1109/IAS.2009.279.

[16] Tezuka, S. (1995). Derandomization. In *Uniform Random Numbers* (pp. 161-192). Springer, Boston, MA.
https://doi.org/10.1007/978-1-4615-2317-8_3.

[17] Fuller, A. T. (1976). The period of pseudo-random numbers generated by Lehmer's congruential method. *The Computer Journal*, *19*(2), 173-177. https://doi.org/10.1093/comjnl/19.2.173

[18] Stipčević, M., & Koç, Ç. K. (2014). True random number generators. In *Open Problems in Mathematics and Computational Science* (pp. 275-315). Springer, Cham. DOI: 10.1007/978-3-319-10683-0_12

[19] Haahr, M. (1998) Random.org – True random number service. Retrieved on 28 may 2021 from www.random.org.

[20] Zhu, Y., & Pei, D. (2002). An algorithm for DLP on anomalous elliptic curves over F p. *Science in China Series A: Mathematics*, *45*(6), 773-777.
https://doi.org/10.1360/02ys9084

[21] Sutherland, A. V. (2012). Identifying supersingular elliptic curves. *LMS Journal of Computation and Mathematics*, *15*, 317-325.
DOI: https://doi.org/10.1112/S1461157012001106

Received February, 2021
Revised May, 2021