Secret sharing schemes from topological spaces

Lakoa Fitina
KnoxMcKen

Abstract

A secret sharing scheme is a method of dividing up a secret into shares, and the shares distributed to participants, such that only authorized subsets of participants can reconstruct the secret when they combine their shares. Many secret sharing schemes have been proposed, since their introduction by Blakley (1979) and Shamir (1979). In Bouroubi et al (2019), set partitions were suggested as a basis for creating a secret sharing scheme. In this paper, we propose several schemes based on the partition of a topological space.

Keywords: secret, sharing, scheme, topological space

Introduction

A secret sharing scheme (SSS) is a method of subdividing a secret into shares and distributing the shares among a set of participants, such that only authorized subsets of participants can reconstruct the secret when they combine their shares. When an unauthorized subset of participants combines their shares they should not be able to reconstruct the secret.

Let X be a non-empty finite set. A topology on X is a set of subsets τ of X, such that X and $\emptyset$ belong to τ, unions of sets in τ are in τ and intersections of elements of τ are in τ. Elements of τ are called open sets. The ordered pair (X, τ) is then called a topological space. Since X is finite, such a space is also called a Kolmogorov space.

A basis for a topological space is a collection of open subsets of the topological space, such that every open subset can be expressed as a (possibly empty) union of basis subsets.

A subset D of X is called dense if D has a nonempty intersection with every nontrivial open set in X.

For example, suppose X = 12345 and $\tau = \{\emptyset, X, \{1, 2, 3\}, \{3, 4, 5\}, \{3\}\}$. Then the set {2, 3, 4} is dense since it intersects non trivially with each nontrivial open set in the space X. Also, {1, 3, 5} is dense.

As another example of a topological space, let X = R be the set of real numbers. An open interval in R is a set (a, b) of real numbers x, such that $a < x < b$. Define a set A to be open, if, for each element p in the set A, there is an open interval (a, b), such that $p \in (a, b) \subseteq A$. The set of all open sets defined this way is a topology on R. So R with all such sets is a topological space. ($\emptyset$ is vacuously open).

If (X, τ) is a topological space and $A \subseteq X$, then a topology can be defined on A, by

$$\tau A = \{A \cap O : O \in \tau\}.$$

τA is called the subspace topology of A, and $(A, \tau A)$ is called a subspace of (X, τ).

A group consists of a set G /= ∅ and a binary operation ∗: G × G → G that is associative, for which there is an identity element, say e, and such that every element in G has an inverse. By associative we mean that a ∗ (b ∗ c) = (a ∗ b) ∗ c for every three elements a, b, c in G. By identity element we mean there is an element e in G such that a ∗ e = a = e ∗ a for every element a in G. By an inverse element, we mean that for every element a in G there is an element a−1 also in G such that a ∗ a−1 = e = a−1 ∗ a. a−1 is called the inverse of a in G. A subset H of a group G is a subgroup of G if it is a group with respect to the binary operation ∗ on G. In this case, we write H ≤ G.

A group G is said to act on a nonempty set X when there is a map ϕ: G × X → X such that (1) ϕ(e, x) = x for every e in G, and (2) ϕ(g, ϕ(h, x)) = ϕ(gh, x) for all g, h in G. The two conditions may be rewritten as ϕ(e, x) = e.x = x and (2) ϕ(g, ϕ(h, x)) = g.(h.x) = (g.h).x. If g ∈ G and x ∈ X then g.x is called the action of g on x. If G acts on X we call X a G-set.
If x and y are two elements in a G-set X, for some group G, then y is in the orbit of x in X, denoted Orb(x) if there is a group element g such that g.x = y.

It is known that (Fraleigh, 2004):

Theorem 1.1. Let G be a group, and X be a G-set. Then the set of orbits in X forms a partition of the set X.

If H is a subgroup of a group G and a ∈ G, a left coset of H with respect to a, is the set

$$aH = \{a * h : h \in G\}.$$

Right cosets are similarly defined. If aH = Ha for all elements a in G, then H is called a normal subgroup. The set of all cosets of a normal subgroup H is denoted by G/H. It turns out that if we define a binary operation (aH).bH) = (a∗ b)H on G/H then G/H becomes a group, called the coset group of G modulo H, or the factor group of G modulo H (Milne, 2021). Here, the identity in this group is H, and the inverse of any element aH is a−1H. Also, if we define a ≈ b iff a and b belong to the same left coset, then ≈ is an equivalence relation on G. Indeed, the left cosets form a partition of G. By Lagrange's theorem, any two left cosets have the same cardinality (Milne, 2021).

In the next section, we discuss creating secret sharing schemes based on finite topological spaces. As far as we know there are no secret sharing schemes created or suggested based on topological space.

Essentially, the secret will be the topology τ on X. However, as we will see later, there are subsets of X that will determine the topology uniquely. Such a subset will be called a share-set. The shared space will be the set of subsets in the share set. Such schemes will be secure because the number of topologies on a large-sized set is not trivial. Suppose that T (n) is the number of topologies on a set of n elements. For small values of n, T (n) has been estimated as follows: T (1) = 1, T (2) = 4, T (3) = 29, T (4) = 355, T (5) = 6, 942, T (6) = 209, 527, T

(7) = 9, 535, 241, (Chaterji, 1966). According to Krishnamurthy (1966), T (n) ≤ 22n−2, n ≥ 1. As yet there is no known general method for obtaining T (n).

Secret Sharing Schemes

Secret sharing schemes are used to increase the security of critical data. This involves the sharing of a secret key between a group of participants by a dealer, such that specific subgroups of the shareholders can recover the secret by pooling their shares. In a threshold (t, n) scheme a dealer distributes a secret value S to 'n' players such that at least t players are required to reconstruct the secret.

The first secret sharing schemes were introduced independently by Blakely (1979) and Shamir (1979). Blakely's scheme was based on the fact that any n nonparallel (n − 1)-dimensional hyperplanes intersect at a specific point. One of the coordinates of this point is taken to be the secret. Each participant is given enough information to define a hyperplane: the secret is then calculated by determining the point of intersection of the hyperplanes, and then taking a specified coordinate of the point of the intersection.

Shamir's scheme is a (t, n) threshold scheme. The scheme relies on the fact that it takes t points to define a polynomial of degree t − 1. The secret is the first coefficient. The shares are the coefficients of the polynomial. When t participants combine their shares, there will be enough information to construct a t − 1 degree polynomial.

Amos Beinel's survey (Beinel, 2011) lists numerous schemes, and we refer the reader to this article for more examples of such schemes.

Secret sharing schemes based on basis sets

In this case, the secret is τ, whereas the shares are the elements of the basis, B. Often, τ can be uniquely determined by a smaller set of subsets of X, for example, the basis.

Example 2.1. Suppose that X = {1, 2, 3, 4, 5, 6}. A topology on X is
τ = {X, ∅, {1, 2, 3, 4, 5}, {1, 2, 3, 4}, {3, 4, 5, 6}, {3, 4, 5}, {1, 2, 5}, {1, 2}, {3, 4}, {5}}.

{{5}, {1,2}, {3,4}, {3,4,5,6}} is the secret.

A basis for this topology, is B = {{5}, {1, 2}, {3, 4}, {3, 4, 5, 6}}. Note that this is a minimal basis, in that no subset of this set is also another basis for the topology. B is the secret.

The above scheme can be modified as follows:

Secret sharing schemes based on Cosets

Suppose that X is a group, and H is a normal subgroup of X. Then the set of left cosets of H partition X. We take the topology in this case to be that generated by these cosets. That is, every element of the topology can be generated, by taking unions, of cosets. This set of cosets is the share-set. That is, the set of left cosets forms the basis for the topology.

Example 2.2. Let X = {0, 1, 2, 3, 4, 5, 6, 7}. This is a group with addition modulo 8, as shown in the group table below:

Table 1: Group with addition modulo 8

$+_8$	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
0	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
1	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*0*
2	*2*	*3*	*4*	*5*	*6*	*7*	*0*	*1*
3	*3*	*4*	*5*	*6*	*7*	*0*	*1*	*2*
4	*4*	*5*	*6*	*7*	*0*	*1*	*2*	*3*
5	*5*	*6*	*7*	*0*	*1*	*2*	*3*	*4*
6	*6*	*7*	*0*	*1*	*2*	*3*	*4*	*5*
7	*7*	*0*	*1*	*2*	*3*	*4*	*5*	*6*

A subgroup in this case is H = {0, 2, 4, 6}. Its cosets are as follows:

1. 0 + H = H = 2 + H = 4 + H = 6 + H = {0, 2, 4, 6}.
2. 1 + H = 3 + H = 5 + H = 7 + H = {1, 3, 5, 7}.
3.

There are only two cosets, but these form the basis or share-set. That is, there are only two shares in this scheme. The secret, in this case, is {{0, 2, 4, 6}, {1, 3, 5, 7}}.

Secret sharing scheme over a subspace topology

Recall that if (X, τ) is a topological space, then a set D ⊆ X is dense, if D has a non-empty intersection with every non-empty open set in the space. The set τD consisting of all the intersections of D with the elements of τ forms a topology on D. That is, (D, τD) is itself a topological space, often referred to as a subspace of (X, τ). In this case, τD is the secret, and the share-set is a minimal basis for τD.

Example 2.3. Let X = {1, 2, 3, 4, 5, 6}. Let τ = {X, ∅, {1, 2, 3, 4, 5}, {1, 2, 3, 5, 6}, {1, 2, 3, 5}, {1, 2, 3, 6}, {3, 4, 5, 6}, {1, 2, 3}, {3, 4, 5}, {3, 5, 6}, {3, 5}, {3, 6}, {3}, {5}, {6}}.

A dense set is D = {2, 3, 5, 6}. To create a topology on D, we take the intersection of D with every nonempty open set and then add on the empty set. We get

τD = {D, ∅, {2, 3, 5}, {2, 3, 6}, {3, 5, 6}, {2, 3}, {3, 5}, {3, 6}, {5, 6}, {3}, {5}, {6}}

It is easy to verify that τD is a topology on D. We now need a basis for this topology, which will become the secret. Such a set is a basis for the subspace topology

B = {{3}, {5}, {6}, {1,2, 3}}

The secret in this case is the set B.

Secret sharing schemes based on group actions

Suppose that G is a group and X is a G-set. By Theorem 1.1, X is partitioned by the action: specifically, the orbits induced by the action will partition X. These orbits will form the basis,

and therefore the share-set of the secret sharing scheme. The set of orbits of X under the action of G, is denoted by X/G.

Example 2.4. Let X = {1, 2, 3, 4, 5, 6}. The set of permutations of the elements of X form a group, denoted by S6 and called the symmetry group on 6 elements. Suppose now that we define the permutation σ: X → X, as follows:

$$\sigma = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{matrix}$$

This means that: σ(1) = 2, σ(2) = 4, etc. Then with regard to orbits, Orb(1) = {1, 2, 4}, Orb(3) = {3, 6} and Orb(5) = {5}. These orbits partition X. But this gives us a basis for a topology. That is the basis is B = {{1, 2, 4}, {3, 6}, {5}}, and this forms the secret.

Example 2.5. Let X = {1,2,3,4,5,6,7,8,9,10,11,12}. A basis is {{1,2}, {3,4}, {5,6},{7,8}, {9,10,11,12}}. The secret in this case is B = {{1,2}, {3,4}, {5,6},{7,8}, {9,10,11,12}}.

Security of the Above Schemes

Various secret sharing schemes were developed since Shamir (1979) proposed one in 1979. The security of the above secret sharing schemes proposed is proportional to the number of topologies that can be defined on a set of n elements, n being a positive integer. In each case, the secret is the topology whereas the set of shares is the basis of the topology. In this section, we will consider the security of these secret sharing schemes based on these assumptions.

According to Krishnamurthy (1966), $T(n) \leq 2^{2^n-2}$, $n \geq 1$. As yet there is no known general method for obtaining $T(n)$.

It has been determined that the number of distinct topologies on a set of n elements, for $1 \leq n \leq 10$, is as follows (see [16]):

Table 2: Number of distinct topologies on a set of n elements

n	Distinct topologies	Inequivalent topologies
0	1	1
1	1	1
2	4	3
3	29	9
4	355	33
5	6942	139
6	209527	718
7	9535241	4535
8	642779354	35979
9	63260289423	363083
10	8977053873043	4717687

In forming a secret sharing scheme based on one of the methods given above, we suggest that a fairly large set be used, as the base set. As can be seen in the above table, for n = 10, the

number of distinct topologies on such a set is already astronomical. We suggest that this therefore makes such a secret sharing scheme secure. The challenge would be to find a basis for the chosen topology.

Conclusion

In this paper we have shown how to create a secret sharing scheme from a finite topological space, using the basis as the share-set. Although a basis for a topology is not unique, a topology generated by a basis is unique. But how does one determine a basis for a given, finite but very large topology? We believe that this is a question worth pursuing.

References

Beimel, A. (2011). Secret-sharing schemes: A survey, In Chee, Y.M., *et al. Coding and Cryptology. IWCC 2011. Lecture Notes in Computer Science*, 6639. https://doi.org/10.1007/978-3-642-20901-7_2

Benoumhani, M. (2006). The number of topologies on a finite set. *Journal of Integer Sequences*, *9*(2), 1-9.

Bouroubi, S., Charhali, F., & Tani, B. (2019). Set partitions: A solution for sharing secret keys. *Romanian Journal of Mathematics and Computer Science*, 9(2), 78-86.

Burnside, M. (1897). Theory of groups of finite order, Cambridge University Press.

Chaterji, S. N. (1966). *The number of topologies on n points*, OEIS, https://oeis.org/A000798/a000798_10.pdf

Fitina, L., Russell, K., & Seberry, J. (2007). The power and influence in some Youden squares and secret sharing. *Utilitas Mathematica*, 73, 143-157.

Fraleigh, J. B. (2004). *A first course in abstract algebra* (7th ed.). Pearson Education.

Ito, M., Saito, A., & Nishizeki, T. (1989). Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan*, 72(9), 56-64.

Itoh, U., & Tochikubo, K. (2019). Recursive general secret sharing scheme based on authorized subsets. *International Journal of Machine Learning and Computing*, 9(1), 1-8.

Krishnamurthy, V. (1966). On the number of topologies on a finite set. *The American Mathematical Monthly*, *73*(2), 154-157.

Mashhour, A., El-Mosef, A., & Farran, A. S. (1986). On the number of topologies on a finite set. *Delta Journal of Science*, *10*(1), 41-65.

Milne, J. S. (2021). Group Theory. Mathematical Site J.S Milne. https://www.jmilne.org/math/CourseNotes/gt.html

Shailesh, A., & Sirali, S. A. (2017). Groups associated with conics. *The Mathematical Gazette*, *93*(526), 27-41.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612-613.

Sloane, N. J. A. (1996). Handbook of integer sequences: Encyclopedia of Integer Sequences. Creative Commons CC BY-SA.

Acknowledgement

I would like to thank Dr Martin Daniel for reviewing this paper. However, responsibility for any errors of fact or opinion remains with the author.

Authors

Lakoa Fitina is a Professor in the Department of Mathematics and Computer Science at Divine Word University. He has an interest in the mathematics of cybersecurity and in studying how pure math subjects can help us understand the problem of data security. Email: Lfitina@dwu.ac.pg.

Knox McKen is interested in cybersecurity, especially in the mathematics of cybersecurity. He is a young and enthusiastic student of mathematics and computer science. Linkedin: linkedin.com/in/knox-mcken-58890836.