ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

A Secret Sharing Scheme Based on a Symmetric $(v, k, \lambda)-$Design

Selda Çalkavur

Abstract: *A $(m, n)-$threshold secret sharing scheme is a method for distributing a secret amongst a group of participants. In a $(m, n)-$threshold secret sharing scheme any m participants recover the secret, but no $(m-1)$ participants can [6]. Each of participants is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together [2]. In this paper, we propose a secret sharing scheme based on a symmetric $(v, k, \lambda)-$design. Then we call it a $(v-k-\lambda, v)-$threshold secret sharing scheme. Morever, we can say the secret sharing scheme is democratic of degree 2.*

Index Terms: Secret sharing, $(m, n)-$threshold secret sharing scheme, projective geometry, symmetric design.

I. INTRODUCTION

Secret sharing schemes were studied by Blakley [1] and Shamir [6] in 1979. In a secret sharing scheme there are one dealer and n participants. Shamir's Secret Sharing Scheme is a $(m, n)-$threshold secret sharing scheme. A $(m, n)-$threshold secret sharing scheme is a method to distribute a secret among n participants in such a way that any m participants can recover the secret, but no $(m-1)$ participants can [6]. A secret sharing scheme is democratic of degree t every group of t participants is in the same number of minimal access sets, where $t \geq 1$ [9]. Projective geometry provides the mathematical structure in order to work out several algorithms [8]. The symmetric design is a projective geometry. So in this work, we construct a secret sharing scheme based on a symmetric $(v, k, \lambda)-$design.

II. SHAMIR'S SECRET SHARING SCHEME

Shamir's Secret Sharing Scheme based on polynomial interpolation. It's a $(m, n)-$threshold scheme. In this scheme, a dealer distribute a secret s to n participants. The goal of this scheme is share secret s among n participants $P_1, P_2, \cdots, P_n$ such that at least m participants are required to reconstruct the secret s. In order to distribute the secret, the dealer chooses a polynomial $f(x)$ of degree $(m-1)$ such that $f(0)=s$. Then the dealer gives the value $s_i = f(i)$ $(i=1, 2, \cdots, n)$ secretly to participant P_i. To recover the secret the participants use polynomial interpolation to recover $f(x)$ and hence the secret is $f(0)$ [2]. In this case no $(m-1)$ participants can obtain any information about the secret while any m of them can [6], [7].
Now we remind some definitions about the secret sharing schemes.

Definition 2.1. ***(Support of a Vector)*** The set $S=\{0 \leq i \leq n-1 \,|\, c_i \neq 0\}$ is called support of a vector $c = c_1 c_2 \ldots c_n \in (F_q)^n$. A codeword c_2 covers a codeword c_1 if the support of c_2 contains that of c_1 [5].

Definition 2.2. ***(Minimal Codeword)*** A minimal codeword c is a codeword which covers just only scalar multiples [5].

Definition 2.3. ***(Minimal Access Set)*** A subset of participants is called a minimal access set, if the participants in the subsets can recover the secret by combining their shares but any subset at the participants can not do so [5].

Definition 2.4. ***(Access Structure)*** The access structure of a secret sharing scheme is the set of all minimal access sets [5].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Definition 2.5. ***(Democratic of Degree)*** A secret sharing scheme democratic of degree t if every group of t participants is in the same number of minimal access sets, where $t \geq 1$ [9].

III. PROJECTIVE GEOMETRIES

A projective geometry of dimension m over a field F is the collection of subspaces of a vector space V of dimension $(m+1)$ over F. The points are the $1-$dimensional subspaces of V, the lines are the $2-$dimensional subspaces,…, the projective $j-$dimensional subspaces,…, the hyperplanes are the $m-$ dimensional subspaces are the elements of the geometry [4].

Example 3.1. Let $F = F_q$. The points and hyperplanes of a projective geometry of dimension m over F form a symmetric design (when $m \geq 2$) with parameters $(q^m + \ldots + q + 1, q^{m-1} + \ldots + q + 1, q^{m-2} + \ldots + q + 1)$. The order of the symmetric design is denoted by $PG(m, q)$ [4]. A projective geometry of dimension 2 is called a projective plane. The parameters of $PG(2, q)$ are $(q^2 + q + 1, q + 1, 1)$. The symmetric $(7, 3, 1)-$ design is isomorphic to $PG(2, 2)$ [4].

Symmetric Designs

An incidence structure consists of a set of points and a set of blocks. There is a relation of incidence between points and blocks.

Definition 3.2. ***(A Symmetric*** $(v, k, \lambda)-$ ***Design)*** A symmetric $(v, k, \lambda)-$design consists of a set P of v points and a set of v subsets of P called blocks such that

- **i)** each block contains exactly k points,
- **ii)** each point lies in exactly k blocks,
- **iii)** each pairs of points occurs together in exactl1y λ blocks,
- **iv)** intersection of each pair of blocks contain exactly λ points.

We denote the set of blocks by B [3].

IV. A SECRET SHARING SCHEME BASED ON A SYMMETRIC $(v, k, \lambda)-$DESIGN

In this section, we construct the secret sharing scheme based on a symmetric $(v, k, \lambda)-$design. We know that the symmetric design is denoted by $PG(m, q)$. Thus we use the projective space $PG(m, q)$.

Consider a symmetric $(v, k, \lambda)-$design D. Let P be the set of points and B be the set of blocks of D. We also know that $|P| = v$ and $|B| = v$. Choose a point in P to be the secret. Call it x_1. The blocks consist of the access structure of this secret sharing scheme. Distribute as shares the set of blocks not containing x_1. By Definition 3.2, point x_1 is incident with k blocks and any two points occurs together in exactly λ blocks. So, there are $(v-k-\lambda)-$blocks both not containing x_1 and any two points not occuring together.

Consider $(v-k-\lambda)-$blocks who will combine their shares and let H be the set of combining. The points compute P/H to find x_1. That is find

$$P/H = \{x_1\}.$$

So, the secret is recovered.

4.1. *A* $(v-k-\lambda, v)-$ *Threshold Secret Sharing Scheme*

We have constructed the secret sharing scheme based on a symmetric $(v, k, \lambda)-$design. In the secret sharing scheme, when any $(v-k-\lambda)$ blocks from v blocks who will combine their shares can recover the secret. So, we call it a $(v-k-\lambda, v)-$threshold secret sharing scheme.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Also, in the secret sharing scheme based on a symmetric $(v, k, \lambda)-$design any two points occur together in exactly λ blocks. Thus, we can say the secret sharing scheme based on a symmetric $(v, k, \lambda)-$design is democratic of degree 2.

Example 4.1. Consider the symmetric $(7, 3, 1)-$design. The set of points of this design is $P=\{0, 1, 2, 3, 4, 5, 6\}$. So $|P|=7$. The set of blocks of this design are
$B_1=\{1, 2, 4\}$, $B_2=\{2, 3, 5\}$, $B_3=\{3, 4, 6\}$, $B_4=\{4, 5, 0\}$, $B_5=\{5, 6, 1\}$, $B_6=\{6, 0, 2\}$, $B_7=\{0, 1, 3\}$.

There are 3 elements in every block. Choose a point in P to be secret. Call it 1. Point 1 is incident with $k=3$ blocks and any two points are incident with $\lambda=1$ block. So, there are $v-k=7-3=4$ blocks not containing 1. These blocks are $B_2=\{2, 3, 5\}$, $B_3=\{3, 4, 6\}$, $B_4=\{4, 5, 0\}$, $B_6=\{6, 0, 2\}$. This means there are $v-k-\lambda=7-3-1=3$ blocks both not containing 1 and any two points not ocuuring together.

Consider $v-k-\lambda=7-3-1=3$ blocks who will combine their shares: Let B_2, B_3, B_4 be these blocks.

$$H=B_2\cup B_3\cup B_4=\{2, 3, 5\}\cup\{3, 4, 6\}\cup\{4, 5, 0\}=\{0, 2, 3, 4, 5, 6\}$$

Compute P/H to find 1. So

$$P/H=\{0, 1, 2, 3, 4, 5, 6\}/\{0, 2, 3, 4, 5, 6\}=\{1\}$$

Hence, the secret is recovered.

V. CONCLUSION

In this work, proposed a secret sharing scheme based on a symmetric $(v, k, \lambda)-$design. This scheme has the same distributed secret as Schamir's Scheme does. So, it is called the $(v-k-\lambda, v)-$threshold secret sharing scheme. Morever, obtained the secret sharing scheme based on a symmetric $(v, k, \lambda)-$design is democratic of degree 2.

REFERENCES

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

[2] Habeeb, M., Kahrobaei, D. and Shpilrain, V., "A Secret Sharing Scheme Based on Group Presentations and the World Problem".

[3] Hill, R. "A First Course in Coding Theory", Oxford: Oxford University, 1986.

[4] Lander, E. S., "Symmetric Designs an Algebraic Approach", Cambridge: Cambridge University, 1983.

[5] Özadam, H., Özbudak, F., Saygı, Z., "Secret Sharing Schemes and Linear Codes", Information Security Cryptology Conference with International Participation, Proceedings, December 2007, pp.101-106.\

[6] Shamir, A., "How to Share a Secret", Commun Assoc. Comp. Mach., vol. 22, 1979, pp.612-613.

[7] Stinson, D. R., "Cryptography: Theory and Practice", Chapman and Hall, 2006.

[8] Venter, A., "Secret Sharing Schemes: An Application of Projective Geometry to Cryptography", May 5, 2005.

[9] Yuan, J., Ding, C., Senior Member, IEEE, "Secret Sharing Schemes from Three Classes of Linear Codes", IEEE Trans. on Inf. Theory, vol. 52, no. 1, January 2006, pp.206-212.

AUTHOR BIOGRAPHY

Selda Çalkavur received Doctor degree from İstanbul Kültür University, İstanbul, Turkey in 2010. She has been working as an assistant professor at Kocaeli University, Kocaeli, Turkey since 2011. She has became a board member in 2011, head of department in 2012 and a vice manager in 2013 at Kocaeli University. Her research interests include coding theory, cryptography, design theory and algebra.