Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090432

A Secret Sharing Scheme based on Residue Class Ring

Selda Çalkavur[*]

Department of Mathematics, Kocaeli University, 41135 Kocaeli, Turkey

Received: 2 Nov. 2014, Revised: 2 Feb. 2015, Accepted: 3 Feb. 2015
Published online: 1 Jul. 2015

Abstract: A (t,n)- threshold secret sharing scheme is a method for distributing a secret amongst a group of participants [1]. Each of participants is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together [6]. In this paper, we propose a secret sharing scheme based on residue class ring $F_p[x]/(f)$, where p is a prime and $deg(f)=n$. Then we call it a $(p^n-1,p^n)-$ threshold secret sharing scheme.

Keywords: Secret sharing, (t,n)- threshold secret sharing scheme, ring, residue class ring.
2000 Mathematics Subject Classification: 14G50, 11T06, 11T71

1 Introduction

Secret sharing has been a subject of study for over 30 years [5]. Shamir [1] studied on the secret sharing schemes in 1979. Shamir's Secret Sharing Sscheme is a (t,n)-threshold secret sharing scheme. Next, we will summarize it.

Secret sharing schemes should be designed as follows:

The first step is to consider a secret space to construct a secret sharing scheme. A secret space consists of the set of participants and a dealer. The dealer has a secret and distributes shares of the secret to each participant. Because if some of the shares of the secret are lost or stolen invalidated, the remaining shares can be modified in a way that the invalid shares cannot be used [3].

In [6] presented two practical secret sharing schemes based on group presentations and the word problem. Their schemes are designed as follows:

The dealer and participants initially are able to communicate over secure channels, but afterwards they communicate over open channels. They first consider the special case where $t=n$. They propose a scheme in which all participants are needed to recover the secret. Then they propose a hybrid scheme that combines Shamir's Scheme and the idea of the (n,n)-threshold scheme.

The theory of rings is a branch of modern algebra [7]. In this work, we mention the rings, polynomials and residue class ring. Then, we construct a secret sharing scheme based on residue class ring using the structures of this ring.

2 Shamir's Secret Sharing Scheme

Shamir's Secret Sharing Scheme based on polynomial interpolation. It's a $(t,n)-$ 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 $P_1,P_2,...,P_n$ such that at least t participants are required to reconstruct the secret s. In order to distribute the secret, the dealer chooses a polynomial $f(x)$ of degree $(t-1)$ such that $f(0)=s$. Then the dealer gives the value $s_i=f(i)$ $(i=1,2,...,n)$ secretly to participant P_i. To recover the secret the participants use polynomial interpolation to recover $f(x)$ and hence the secret $f(0)$ [6]. In this case no $(t-1)$ participants can obtain any information about the secret while any t of them can [1], [3].

Now, we remind some definitions about the secret sharing schemes.

Definition 21*(Support of a Vector) The set $S=\{0\leq i\leq n-1|c_i\neq 0\}$ is called support of a vector $c=c_1c_2...c_n\in(F_q)^n$. A codeword c_2 covers a codeword c_1 if the support of c_2 contains that of c_1 [4].*

Definition 22*(Minimal Codeword) A minimal codeword c is a codeword which covers just only its scalar multiples [4].*

Definition 23*(Minimal Access Set) A subset of participants is called a minimal access set, if the participants in the subsets can recover the secret by*

[*] Corresponding author e-mail: selda.calkavur@kocaeli.edu.tr

combining their shares but any subset at the participants can not do so [4].

Definition 24*(Access Structure) The access structure of a secret sharing scheme is the set of all minimal access sets [4].*

3 Rings and Fields

In this section, we give a minimum information from ring theory necessary to understand our secret sharing scheme.

Definition 31*A ring $(R,+,.)$ is a set R, together with two binary operations, denoted by "+" and ".", such that:*
1) R is an abelian group with respect to "+"
2) "." is associative; that is, $(a.b).c = a.(b.c)$ for all $a,b,c \in R$
3) The distributive laws hold; that is $a.(b+c) = a.b+a.c$ and $(b+c).a = b.a+c.a$ for all $a,b,c \in R$ [7].

Definition 32*1) A ring is called commutative if "." is commutative.*
2) A commutative division ring is called a field [7].

Definition 33*A subset J of a ring R is called an ideal provided J is a subring of R and for all $a \in J$ and $r \in R$ we have $ar \in J$ and $ra \in J$ [7].*

Definition 34*Let R be a commutative ring. An ideal J of R is said to be principal if there is an $a \in R$ such that $J = (a)$. In this case, J is also called the principal ideal generated by a [7].*

Ideals are normal subgroups of the additive group of a ring, so an ideal J of the ring R defines a partition of R into disjoint cosets, called residue classes modulo J. The residue class of the element a of R modulo J will be denoted by $[a] = a+J$.

The set of residue classes of a ring R modulo an ideal J forms a ring with respect to the operations

$$(a+J)+(b+J) = (a+b)+J \tag{3.1}$$

$$(a+J)(b+J) = ab+J \tag{3.2}$$

[7].

Definition 35*The ring of residue classes of the ring R modulo the ideal J under the operations (3.1) and (3.2) is called the residue class ring of R modulo J. It is denoted by R/J [7].*

Example 36*(The residue class ring $Z/(n)$) Denote the coset or residue class of the integer a modulo the positive integer n by $[a]$, as well as by $a+(n)$, where (n) is the principal ideal generated by n. The elements of $Z/(n)$ are $[0]$=0+(n), $[1] = 1+(n)$,..., $[n-1] = n-1+(n)$ [7].*

Theorem 37*$Z/(p)$, the ring of residue classes of the integers modulo the principal ideal generated by a prime p is a field [7].*

Definition 38*For a prime p, let F_p be the set $\{0,1,...,p-1\}$ of integers and let $\varphi : Z(p) \to F_p$ be the mapping defined by $\varphi([a]) = a$ for $a = 0,1,...,p-1$. Then F_p is a finite field, called the Galois field of order p [7].*

3.1 Polynomials

Let R be an arbitrary ring. A polynomial over R is an statement of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

where n is a positive integer, the coefficients a_i $(0 \leq i \leq n)$ are elements of R and x is a symbol not belonging to R, called an indeterminate over R. The polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ over R are considered. It defines the sum of $f(x)$ and $g(x)$ by

$$f(x)+g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

The polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^i$ over R are considered. The product of two polynomials over R is

$$f(x).g(x) = \sum_{k=0}^{n+m} c_k x^k,$$

where $c_k = \sum_{i+j=k} a_i b_j$ $(0 \leq i \leq n,\ 0 \leq j \leq m)$ [7].

Definition 39*The ring formed by the polynomials over R with the above operations is called the polynomial ring over R and denoted by $R[x]$ [7].*

Theorem 310*For $f \in F[x]$, the residue class ring $F[x]/(f)$ is a field if and only if f is irreducible over F [7].*

Consider the residue class ring $F[x]/(f)$, where f is an arbitrary nonzero polynomial in $F[x]$. The $F[x]/(f)$ is exactly the residue class $r+(f)$, where r runs through all polynomials in $F[x]$ with $deg(r) < deg(f)$. Thus, if $F = F_p$ and $deg(f) = n \geq 0$, then the number of elements of $F_p[x]/(f)$ is equal to the number of polynomials in $F_p[x]$ of degree$<n$, which is p^n.

Example 311*i) Let $f(x) = x \in F_2[x]$. The $p^n = 2^1$ polynomials in $F_2[x]$ of degree <1 determine all residue classes comprising $F_2[x]/(x)$. Thus, $F_2[x]/(x)$ consists of the residue classes $[0]$and $[1]$ and isomorphic to F_2.*
ii) Let $f(x) = x^2+x+1 \in F_2[x]$. Then $F_2[x]/(f)$ has the $p^n = 2^2$ elements $[0],[1],[x],[x+1]$ [7].

4 A Secret Sharing Scheme Based on Residue Class Ring

In this section, we construct a secret sharing scheme based on residue class ring.

Consider the residue class ring $F_p[x]/(f)$, where p is a prime and $deg(f) = n$. The number of elements of $F_p[x]/(f)$ is equal to the number of polynomials in $F_p[x]$ of degree$< n$, which is p^n. Let the residue class ring $F_p[x]/(f)$ be the participants set in this secret sharing scheme. The dealer chooses a residue class in $F_p[x]/(f)$ to be the secret. Call it $[s]$. So, the secret is recovered as follows:

We know that the sum of p^n residue classes is

$$[k_1]+[k_2]+...+[k_{p^n}] \equiv 0(mod\ p).$$

Now, (p^n-1) residue classes will combine their shares, that is

$$[k_1]+[k_2]+...+[k_{p^n}-1]+[s] \equiv 0(mod\ p).$$

The secret is recovered by solution of above equation.

4.1 The (p^n-1,p^n)- Threshold Secret Sharing Scheme

We have proposed a secret sharing scheme based on residue class ring. In this secret sharing scheme, there are p^n participants. Any (p^n-1) of the participants can recover the secret. So, we call it the (p^n-1,p^n)-threshold secret sharing scheme.

Example 41*Let $f(x) = x^3+x \in F_2[x]$. The $p^n = 2^3$ polynomials in $F_2[x]$ of degree<3 determine all residue classes comprising $F_2[x]/(x^3+x)$. Then,*

$$F_2[x]/(x^3+x) = \{[0],[1],[x],[x^2],[x+1],[x^2+1],[x^2+x],[x^2+x+1]\}.$$

Now, choose a residue class in $F_2[x]/(x^3+x)$ to be secret. Call it $[s]=[x+1]$. So, 8-1=7 residue classes will combine their shares as follows:

$$[0]+[1]+[x]+[x^2]+[x^2+1]+[x^2+x]+[x^2+x+1]+[s] \equiv 0(mod\ 2)$$

$$[x+1]+[s] \equiv 0(mod\ 2)$$

$$[s]=[x+1]$$

Hence, the secret is recovered.

5 Conclusion

In this work, proposed a secret sharing scheme based on residue class ring. This scheme has the same distributed secret as Shamir's Scheme does. So, it is called (p^n-1,p^n)- threshold secret sharing scheme. This scheme has the following useful advantages over Shamir's Scheme: While recovering the secret (p^n-1) out of p^n residue classes combine their shares. That is the access structure of this secret sharing scheme is reliable. p and n can be large numbers. It is not important. Because, for example if p=2 and n=128, then there will be 2^{128} participants in that secret sharing scheme. While recovering the secret $(2^{128}-1)$ out of 2^{128} participants combine their shares. That is the number of participants in the access structure is too much. So, this means it is reliable of this scheme.

Acknowledgement

The author would like to thank to Maggie Habeeb, Delarom Kahrobaei and Vladimir Shpilrain for their valuable paper is called "A Secret Sharing Scheme Based on Group Presentations and the Word Problem".

References

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

[2] C. Chames, J. Pieprzyk, R. S. Naini, "Conditionally Secure Secret Sharing Schemes with Disenrollment Capability", Proceedings of the 2^{nd} ACM Conference on Computer and Communications Security, Fairfax, Virginia, US, November 2-4, 1994.

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

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

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

[6] M. Habeeb, D. Kahrobaei and V. Shpilrain, "A Secret Sharing Scheme Based on Group Presentations and the Word Problem", Contemp. Math. Amer. Math. Soc. pp. 143-150, 582 (2012).

[7] R.Lidl, H. Niederreiter, "Finite Fields", vol. 20, Cambridge.

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 director in 2013 at Kocaeli University. Her research interests include coding theory, cryptography, design theory, algebra.