Secret Sharing, Zero Sum Sets, and Hamming Codes

Selda Çalkavur [1] and Patrick Solé [2],*

[1]   Mathematics Department, Kocaeli University, 41380 Kocaeli, Turkey; selda.calkavur@kocaeli.edu.tr
[2]   I2M, Aix Marseille University, Centrale Marseilles, CNRS, 163 Avenue de Luminy, 13009 Marseille, France
*   Correspondence: sole@enst.fr

Abstract: A (t, n)-secret sharing scheme is a method of distribution of information among n participants such that any $t > 1$ of them can reconstruct the secret but any $t - 1$ cannot. A ramp secret sharing scheme is a relaxation of that protocol that allows that some $(t - 1)$-coalitions could reconstruct the secret. In this work, we explore some ramp secret sharing schemes based on quotients of polynomial rings. The security analysis depends on the distribution of zero-sum sets in abelian groups. We characterize all finite commutative rings for which the sum of all elements is zero, a result of independent interest. When the quotient is a finite field, we are led to study the weight distribution of a coset of shortened Hamming codes.

1. Introduction

Secret sharing schemes were introduced by Shamir in 1979 [1]. A (t, n)-secret sharing scheme is a method of distribution of information among n participants such that $t > 1$ can reconstruct the secret but any $t - 1$ cannot.

The person distributing the shares is called the dealer and a minimal t-subset of participants that can reconstruct the secret is called a coalition. Shamir scheme was based on polynomial interpolation but was later shown by McEliece and Sarwate to be an application of the Massey scheme, a scheme based on codes [2], to Reed-Solomon codes [3].

In the present work, we present a ramp secret sharing scheme based on polynomial residue rings. It was shown in [4] that such schemes can be concatenated with a classical (t, n)-scheme. Thus, our scheme complements but does not compete with Shamir scheme for instance. We generalize and sometimes correct the results of [5]. To determine the residue rings where our scheme can be applied, we are led to characterize all finite commutative rings that are S_0. These are defined by the property that the sum of all their elements is zero. This result is of independent algebraic interest. When the residue ring is a finite field, to study the size distribution of admissible coalitions, we are led to study the weight distribution of a coset of shortened Hamming codes. The analysis employs the MacWilliams formula and the fact that Hamming codes are homogeneous.

The material is organized as follows. Section 2 discusses S_0 rings. Section 3 describes the scheme, and analyzes its security. Section 4 collects concluding remarks and open problems.

2. Algebraic Preliminaries

The aim of the first three subsections is to characterize commutative rings for which the sum of all elements is zero.

2.1. Integer Residue Rings

We begin with a lemma on integer residues.

Lemma 1. *If N is an odd integer, then $\sum_{i=1}^{N} i$ is an integer divisible by N.*

Proof. Summing an arithmetic series yields $\sum_{i=1}^{N} i = \frac{N(N+1)}{2}$. Since N is odd, the number $\frac{(N+1)}{2}$ is an integer. $\square$

Remark 1. *Note that the result does not hold for even integers. For instance, $1 + 2 + 3 + 4 = 10$ is not a multiple of 4. In fact, the sum is congruent to $N/2$ modulo N.*

We proceed to generalized the above result to polynomial residue rings. Let q be an arbitrary integer > 1. Let f denote a polynomial of degree d in $\mathbb{Z}_q[x]$ and denote by $R(f)$ the quotient ring $\mathbb{Z}_q[x]/(f(x))$.

Theorem 1. *If q is odd and $d \geq 1$ or q is even and $d > 1$, then $\sum_{h \in R(f)} h = 0$.*

Proof. If $d = 1$ and q is odd, the preceding Lemma applies with $N = q$. If $d > 1$, write the residue class representative h as

$$h = \sum_{i=0}^{d-1} h_i x^i.$$

We see that, for given i, any fixed value of h_i will appear q^{d-1} times when the h'_js with $j \neq i$ range over $\mathbb{Z}_q$. The result follows since then $d > 1$. $\square$

2.2. Zero-Sum Sets

We want to exhibit $R(f) = \mathbb{Z}_q[x]/(f(x))$ the sum of all elements of which is zero, but without smaller size zero-sum sets. The next result shows that composite q's should be avoided.

Lemma 2. *Assume $d > 1$. If m divides q, then $R(f)$ has a zero-sum set of size m^d.*

Proof. Writing $q = ms$, and $g = f \pmod{m}$, we see that $R(g)$ embeds additively into $R(f)$ by the map $h \mapsto sg$. Thus, $R(f)$ by Theorem 1 applied to $R(g)$ has a zero sum-set of size m^d. $\square$

Next, we show that composite f's should be avoided.

Lemma 3. *Assume $d > 1$. If h of degree $d > s > 1$ divides f, then $R(f)$ has a zero-sum set of size q^s.*

Proof. Writing $f = hr$, and we see that $R(h)$ embeds additively into $R(f)$ by the map $g \mapsto rg$. Thus, $R(f)$ by Theorem 1 applied to $R(h)$ has a zero-sum set of size q^s. $\square$

Eventually, $p^d - 1$ should not be composite.

Lemma 4. *Assume $R(f) = GF(p^d)$ and that $d > 1$. If s divides $p^d - 1$, then $R(f)$ has a zero-sum set of size s.*

Proof. In that case, the multiplicative group of $R(f)$ contains s roots of unity of order s, which add up to zero. $\square$

2.3. Generalization to Rings

Definition 1. *A ring R is S_0 iff*

$$\sum_{x \in R} x = 0.$$

Proposition 1. *If the ring R contains a unit u such that $1 - u$ is also a unit, then R is S_0.*

Proof. Let $S = \sum_{x \in R} x$. Since u is invertible, then the map $x \mapsto ux$ permutes R. Thus, $uS = S$, and so $(1 - u)S = 0$. $\square$

Remark 2. *The condition is sufficient but not necessary as the ring* $\mathbb{F}_2 \times \mathbb{F}_2$ *is* S_0 *and contains only one unit* $u = (1, 1)$. *Thus,* $(1, 1) - u = (0, 0)$, *which is not a unit.*

The following result is well-known.

Corollary 1. *Every finite field* $\mathbb{F}_q$ *except* $\mathbb{F}_2$ *is* S_0.

Proof. If $q > 2$, any nonzero element $u \neq 1$ is such that $1 - u$ is invertible. $\square$

The following result shows that many rings are S_0.

Corollary 2. *Every ring of odd characteristic is* S_0.

Proof. If the characteristic is odd, then $u = 2$ is a unit and also $1 - u = -1$. $\square$

We are still far from a characterization as there are many even characteristic S_0 rings, like e.g., the direct product $\mathbb{F}_2 \times \mathbb{F}_2$. A complete characterization was given in [6]. To be self-contained, we sketch a proof here.

Theorem 2. *A commutative ring is not* S_0 *iff its additive group contains only one summand of even size in its decomposition as a direct sum of cyclic groups.*

Proof. The sum of all the elements of a finite abelian group G is equal to the sum of elements of order 2. Call $\mathcal{N}$ the set consisting of 0 and the elements of order 2. The set $\mathcal{N}$ is an abelian group, or, equivalently, a vector space over $\mathbb{F}_2$, of dimension k, say. Thus, the set of all elements of $\mathcal{N}$ is zero iff it is the case for $\mathbb{F}_{2^k}$. By Corollary 1, this happens iff $k = 1$, iff $|\mathcal{N}| = 2$. Thus, G contains exactly one element of order 2. This happens iff it contains only one summand of even size in its fundamental decomposition as a direct sum of cyclic groups. $\square$

2.4. Secret Sharing Schemes

Definition 2. *(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 of these can not do so [7].*

Definition 3. *(Access Structure) The access structure of a secret sharing scheme is the set of all minimal access sets [7].*

Definition 4. *(Ramp Secret Sharing Scheme) Ramp secret sharing scheme (RSS) is a relaxation of secret sharing scheme. In a RSS of parameters* (m, t, n) *with* $m < t < n$, *all t-subsets can reconstruct the secret, no j-subsets with* $j < m$ *can reconstruct the secret, and some j-subsets with* $m \leq j < t$ *can reconstruct the subset. There is a lot of work on the ramp secret sharing scheme. Some of them are given in [8,9]. Alahmadi et al. [8] explain a multisecret-sharing scheme based on LCD codes. They use Blakley's method to construct their scheme. Çalkavur and Solé [9] introduce some multisecret-sharing schemes over finite fields. In their work, they claim that the Blakley scheme does not work well if they replace* $\mathbb{R}$ *with a finite field. These two schemes are also the ramp secret sharing schemes.*

3. The Scheme

Assume a polynomial residue ring $R(f) = GF(2^d)$ that satisfies the hypothesis of Theorem 1 and construct a threshold scheme based on this ring. Put $n = 2^d$, with $d > 2$. We construct an

$(3, n-1, n-1)$-ramp scheme. The motivation for this special choice of $R(f)$ is as follows. From the three Lemmas above, the recommended values of $R(f)$ in the notation of §II are

1. $q = 2$
2. f irreducible
3. $2^d - 1$ prime
4. $d > 4$.

The primes of the form $2^d - 1$ are called Mersenne primes. The first few admissible d's are $2, 3, 5, 7$. The largest known in April 2020 was for $d = 82{,}589{,}933$ [10]. For that value of d, the quantity $2^d - 1$ is the largest known prime today.

The share dealing protocol proceeds as follows:

- All of the elements of $GF(2^d)$ are written as binary vectors of length d.
- The dealer pics any element of $GF(2^d)$ as the secret.
- He distributes the remaining $n - 1$ elements of $R(f)$ to the $n - 1$ users.

The recovery phase is as follows. The set of all $n - 1$ users pool their shares together, and add them up obtaining a sum Σ. Thus, the secret is then computed as $s = -\Sigma$. We summarize the discussion in the following proposition.

Proposition 2. *With the above conditions, the finite field $GF(2^d)$ determines a $(3, 2^d - 1, 2^d - 1)$-ramp secret sharing scheme.*

Proof. By Corollary 1, the finite field $GF(2^d)$ is S_0. Anticipating the next section, we see that the zero sum sets of $GF(2^d)$ are in bijection with the codewords of the Hamming code of parameters $[2^d - 1, 2^d - 1 - d, 3]$. This means, in the scheme, there are $2^d - 1$ participants, and the secret is split in $2^d - 1$ pieces and there are zero-sum set of size 3 corresponding to weight 3 codewords in Hamming scheme. The results follow. □

3.1. Coding Interpretation

The following result is elementary but essential. A coalition is any zero-sum set containing the secret, minus the secret itself.

Proposition 3. *There is a bijective correspondence between coalitions of size w and codewords of weight $w + 1$ in the Hamming code $\mathcal{H}_d$ of parameters $[n - 1, n - 1 - d, 3]$.*

Proof. Let H be the matrix with columns all the $2^d - 1$ nonzero binary vectors of length d. As is well-known [11], this matrix is a parity-check matrix for the said Hamming code $\mathcal{H}_d$. Let C be a coalition, and let χ_C be the characteristic vector of $C' = C \cup s$, where s denotes the secret. Since C' is a zero-set, we know that $H\chi_C = 0$, implying $\chi_C \in \mathcal{H}_d$. Furthermore, $|C'| = |C| + 1$ equals the Hamming weight of χ_C. □

3.2. Random Choice Attack

An obvious attack is to suppose a coalition with a zero-set containing the secret minus the secret, and let the members of the coalition add up their shares. The following result is immediate by the coding interpretation of Proposition 3. Denote by $\mathcal{H}_d^-$ the code obtained from $\mathcal{H}_d$ by puncturing in an arbitrary position, and only retaining the codewords which were equal to one in that position. In other words, it is the coset of the shortened code into the punctured code at the same position.

Proposition 4. *The probability that a random set of $[1, \ldots, n - 2]$ size w is a coalition is $\frac{A_w}{\binom{n-2}{w}}$, where A_w is the number of codewords of weight w in $\mathcal{H}_d^-$.*

Proof. By Proposition 3, the characteristic vector of a coalition is a codeword of $\mathcal{H}_d^-$, where the puncture has been done at the coordinate place determined by the secret. □

The A_w's can be computed by the generating function:

$$\sum_{w=0}^{n-2} A_w x^{n-1-w} y^w = \frac{1}{n-1} \frac{\partial}{\partial y} W(x,y),$$

(coming from ([12] Th. 3)), where $W(x,y)$, the weight enumerator of $\mathcal{H}_d$, is easily computed by MacWilliams transform:

$$W(x,y) = \frac{1}{2^d} \left((x+y)^{n-1} + (n-1)(x+y)^{n-1-n/2}(x-y)^{n/2} \right),$$

using the fact that the dual of the Hamming code, the so-called Simplex code is a one-weight code ([11] Chap. 5, Prob. 3).

Example 1. *For small values of d, a direct computation in Magma [13] yields the following data. The weight distribution is described as a list*

$$[< 0, 1 >, \ldots, < i, A_i >, \ldots].$$

We consider $d = 3$, when $\mathcal{H}_3$ is a $[7,4,3]$ code.

- The weight distribution of $\mathcal{H}_3$, punctured at coordinate 1 is $[< 0, 1 >, < 2, 3 >, < 3, 8 >, < 4, 3 >, < 6, 1 >]$.
- The weight distribution of $\mathcal{H}_3$, shortened at coordinate 1 is $[< 0, 1 >, < 3, 4 >, < 4, 3 >]$.
- On the contrary, we see that the weight distribution of $\mathcal{H}_3^-$, is $[< 0, 1 >, < 2, 3 >, < 3, 4 >]$.

　　Higher values of d (say e.g., $d = 7$) are feasible but lead to longer formulas.
　　To be concrete, we give a special case.

Proposition 5. *In this scheme, there are $\frac{n}{2} - 1$ coalitions of size 2.*

Proof. By Proposition 3, such an access set is of the form $\{x, x+s\}$, where s is the secret and x is an arbitrary nonzero vector different from s. Replacing x by $x+s$ gives the same set. □

These calculations show that the value of n should be large for the scheme to be secure.

3.3. Information Rate

　　Another important parameter in secret sharing is the information rate ρ of the scheme. It is equal to the ratio of the size of the secret to the maximum size of the pieces of participants [14]. Since the secret is an element of length d in $GF(2^d)$, its size is d. Thus, the information rate is 1.
　　If the information rate is equal to one, then this scheme is called the ideal. Thus, our new scheme is an ideal secret sharing scheme.

3.4. Comparison with Other Schemes

　　Let $\mathbb{F}_{q^n}$ denote the finite extension of degree n of the finite field $\mathbb{F}_q$. Now, we compare our scheme with other ramp type schemes in the Table 1. The number of participants, the size of a secret, and the number of coalitions for an $[n,k]$-code over $\mathbb{F}_{11}$ are denoted by T, R, S, respectively. Moreover, consider a polynomial residue ring $R(f) = GF(2^d)$.

Table 1. Comparison table.

System	[8]	[9]	This Paper
T	q^k	q^n	$2^d - 1$
R	q^n	q	2^d
S	$\dfrac{\prod_{i=0}^{k-1}(q^k - q^i)}{k!}$	$\dfrac{\prod_{i=0}^{n-1}(q^n - q^i)}{n!}$	$\dfrac{2^d - 1}{2} - 1$
ρ	$\dfrac{k}{k+1}$	1	1

3.5. Combination with Shamir's Scheme

The advantage of using a secret with values in a finite field is that it can be used in conjunction with Shamir's scheme which is based on polynomial interpolation over a finite field.

4. Conclusions

In the present article, we have generalized the work [5] to a wider class of quotient rings. Possible attacks have been considered. Secure values of f, n, d have been recommended. Even in the recommended values of the parameters, there are still zero sum-sets of size 2^{d-1}. Moreover, our scheme has the same distributed secret as Shamir's scheme does. We send the residue classes in disguise over open channels and then participants use properties of zero-sum sets to recover the secret. The combined scheme has the following useful advantages over Shamir's original scheme:

- The shares are elements of a polynomial residue ring that can be sent over open channels and then participants use ring-theoretic methods to recover the secret.
- Once the long-term private information (the share) is distributed, several different secrets can be distributed without updating the long-term private information.
- While recovering the secret, if participants do not want to, they do not have to reveal their shares to each other.

On the combinatorial side, it would be interesting to derive an upper bound on the size of nontrivial zero-sum sets in $R(f)$. Characterizing the distribution of zero-sum sets in general commutative rings seems to be a challenging problem in ring theory, as it cannot use the standard decomposition theorems, like CRT and so on.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. Massey, J.L. Minimal codewords and secret sharing. In Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden, 22–27 August 1993.
3. McEliece, R.J.; Sarwate, D.V. On sharing secrets and Reed-Solomon codes. *Commun. Assoc. Comp. Mach.* **1981**, *24*, 583–584. [CrossRef]
4. Habeeb, M.; Kahrobaei, D.; Shpilrain, V. A secret sharing scheme based on group presentations and the word problem. *Contemp. Math. Am. Math. Soc.* **2012**, *582*, 143–150.
5. Çalkavur, S. A secret sharing scheme based on residue class rings. *Appl. Math. Inf. Sci.* **2015**, *9*, 1–3.

6. MathStackExchange Post. Available online: https://math.stackexchange.com/questions/1614276/a-special-class-of-commutative-rings (accessed on 29 February 2020).
7. Özadam, H.; Özbudak, F.; Saygı, Z. Secret Sharing Schemes and Linear Codes. In Proceedings of the Information Security Cryptology Conference with International Participation, Seoul, Korea, 4–6 December 2007; pp. 101–106.
8. Alahmadi, A.; Altassan, A.; AlKenani, A.; Çalkavur, S.; Shoaib, H.; Solé, P. A Multisecret-Sharing Scheme Based on LCD Codes. *Mathematics* **2020**, *8*, 272. [CrossRef]
9. Çalkavur, S.; Solé, P. Some Multisecret-Sharing Schemes over Finite Fields. *Mathematics* **2020**, *8*, 654. [CrossRef]
10. GIMPS Webpage. Available online: https://www.mersenne.org/primes/?press= (accessed on 28 April 2020).
11. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error-Correcting Codes*; North-Holland: Amsterdam, The Netherlands, 1977.
12. Bonnecaze, A.; Mourrain, B.; Solé, P. Jacobi Polynomials, Type II Codes, and Designs. *Des. Codes Cryptogr.* **1999**, *16*, 215–234. [CrossRef]
13. Magma Website. Available online: http://magma.maths.usyd.edu.au/magma/ (accessed on 1 March 2020).
14. Padro, C. Robust vector space secret sharing schemes. *Inf. Process. Lett.* **1998**, *68*, 107–111. [CrossRef]