mathematics

Article

A Multisecret-Sharing Scheme Based on LCD Codes

Adel Alahmadi [1], Alaa Altassan [1], Ahmad AlKenani [1], Selda Çalkavur [2], Hatoon Shoaib [1] and Patrick Solé [3,*]

[1] Math Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia; adelnife2@yahoo.com (A.A.); aaltassan@kau.edu.sa (A.A.); aalkenani10@hotmail.com (A.A.); hashoaib@kau.edu.sa (H.S.)
[2] Math Department, Köseköy Vocational School, Kocaeli University, Kocaeli 41135, Turkey; selda.calkavur@kocaeli.edu.tr
[3] CNRS, Aix Marseille University, Centrale Marseille, I2M, 13009 Marseille, France
* Correspondence: sole@enst.fr

Received: 13 January 2020; Accepted: 12 February 2020; Published: 18 February 2020

Abstract: Secret sharing is one of the most important cryptographic protocols. Secret sharing schemes (SSS) have been created to that end. This protocol requires a dealer and several participants. The dealer divides the secret into several pieces (the shares), and one share is given to each participant. The secret can be recovered once a subset of the participants (a coalition) shares their information. In this paper, we present a new multisecret-sharing scheme inspired by Blakley's method based on hyperplanes intersection but adapted to a coding theoretic situation. Unique recovery requires the use of linear complementary (LCD) codes, that is, codes in which intersection with their duals is trivial. For a given code length and dimension, our system allows dealing with larger secrets and more users than other code-based schemes.

Keywords: secret sharing; multisecret-sharing; linear codes

1. Introduction

Secret sharing schemes (SSS) form one of the key management or establishment schemes introduced independently in 1979 by both Shamir [1] and Blakley [2]. The working principle of these schemes is based on protecting the encryption keys. SSS are also used to save a secret recipe, or a password to a bank vault, check access of nuclear weapons, and more. We need these schemes because many cryptosystems that use one sole master key have various vulnerabilities. For instance, if the main key is accidentally disclosed to the public, this will compromise the entire system. In addition, if the main key is lost, then all the other keys it controls become unattainable. Additionally, if the keeper of the main key turns out to be disloyal, then all sensitive information will be leaked to the opponents [3]. In addition, these schemes are useful when we do not trust a single person owning a certain secret.

The technique of a SSS is to keep the key and then this secret is split into several parts called shares and distributed them among participants. The secret can be reconstructed thanks to the certain subsets of the pieces. The one who produces such pieces and privately delivers them to the participants is called the dealer [4].

SSS have been implemented in different areas, such as Information Security, Threshold Cryptography, Key Recovery Mechanism, Information Hiding, Electronic Voting, and many others [5–7].

Another important class of SSS is multisecret-sharing schemes. Some of them were proposed in [8–13]. There is a set of r secrets in these schemes. Either the r secrets can be shared immediately or all r secrets cannot be recovered [10,11,14]. To reconstruct the secret it is needed that the participants transmit a $pseudo - share$ instead of the secret share itself. This $pseudo - share$ is computed from their secret share.

In this article, we present a new multisecret-sharing scheme based on linear codes. We give its reconstruction algorithm by using Blakley's method. To ensure unique recovery of the secret, we need to assume that the code used is Linear Complementary Dual (LCD). Such codes were studied by Massey in 1992 [15]. Massey constructed some LCD cyclic codes over finite fields as BCH codes [16]. These codes are called reversible codes. LCD codes have enjoyed a renaissance in recent years due to their application to Boolean masking [17], a security countermeasure in embarked electronics. Many constructions of such codes are recognized from either combinatorics [18] or algebraic codes [19]. Yang and Massey found a necessary and sufficient condition for a cyclic code to have a complementary dual [20]. Sendrier showed LCD codes meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes [21]. Esmaeili and Yari examined 1-generator LCD quasi-cyclic codes [22]. Muttoo and Lal explored reversible codes over $GF(q)$ [23]. Tzeng and Hartmann showed the minimum distance of a class of reversible cyclic codes is larger than the BCH bound [24]. A linear programming bound on the largest size of a binary LCD code of given length and minimum distance was derived in [18]. Güneri, Özkaya and Solé also studied quasi-cyclic LCD codes [19]. Carlet and Guilley studied an application of LCD codes against side-channel attacks and explained several constructions of LCD codes [17].

We assayed the security of our scheme by means of linear algebra over finite fields. We counted the size of minimal coalitions in this scheme. Massey's scheme [25], Ding et al.'s [26], and Çalkavur et al.'s [13] are some of code-based schemes in the literature. We conclude the article by a comparison between our scheme and these schemes.

This paper is organized as follows. In Section 2, some facts about linear codes and SSS are introduced. In Section 3, we present the new system and explain its security. In Section 4, we compare our scheme with the other schemes. Finally, Section 5 concludes our work.

2. Background and Preliminaries

In this section, we introduce some principles as a preliminary.

2.1. Linear Codes

Denote the finite field of order q by $\mathbb{F}_q$, where q is a prime power. An $[n,k]-$**code** C over $\mathbb{F}_q$ of length n and dimension k is a subspace in $(\mathbb{F}_q)^n$. The **dual code** of C consists of all vectors in $(\mathbb{F}_q)^n$ that are orthogonal to every codeword of C. This code is denoted by $C^\perp$ and is an $[n, n-k]-$code. One of the important invariants of a linear code C is the generator matrix G. G is a $k \times n$ matrix the rows of which form a basis of C. A generator matrix for the dual code $C^\perp$ is a parity-check matrix H.

The **hull** of a code is the intersection of C with $C^\perp$. If the hull of a code is trivial, this code is **linear complementary dual** (LCD).

2.2. LCD Code

A linear code with complementary code (LCD) is a linear code C satisfying $C \cap C^\perp = \{0\}$. Any code over a field is equivalent to a code generated by a matrix of the form $(I_k|A)$, where I_k denotes the k by k identity matrix [18].

2.3. Overview of Secret Sharing Schemes

Secret sharing is a method by which a dealer distributes shares that are called the pieces of the secret. The main idea is the certain subsets of participants can recover the secret, the others cannot. SSS play an important role for several secure records. Some of them are threshold cryptography, attribute-based encryption, and access control [27].

We will need the following notations to define SSS:

- **Shares** or shadows which are pieces of information. In this SSS, these shares have the property that certain component group of shares can recover the secret, and the other group of shares cannot.
- The set of all possible shares is called the **share set**.
- The **secret** could be a key, or a message, or any valuable information.
- The **participants** are the parties that will receive the pieces.
- The **dealer** who picks the secret key and distributes its pieces among participants.
- The **access structure** is the set of all minimal coalitions sets. The elements in this structure are the authorized combinations of participants whose shares can be used to retrieve the secret.

Thus, we can say that any secret sharing scheme contains the following two phases.

- **Distribution Phase:** The secret is splitted into N shares $y_1, y_2, \cdots, y_N$ that are privately delivered to the participants.
- **Reconstruct Phase:** The secret can be recovered by using a specific algorithm for a suitable set of shares.

2.4. Blakley Secret Sharing Scheme

Blakley's SSS was constructed in 1979. It is based on finite geometry [5]. This scheme uses hyperplane geometry as a solution of the secret sharing problem. Here, the n participants are given a hyperplane equation in a k-dimensional space over a finite field. Thus, a (k, n)-threshold scheme is generated. In some cases, all hyperplane meet through a particular point. The intersection point of the hyperplanes is the secret. Coefficient of hyperplanes corresponds to the shares.

In this approach, the secret and the shares can be considered as a linear system $AX = T$, where the matrix A and the vector T corresponds to hyperplane equations. Once participants need to reconstruct the secret by solving the equation systems [28]. Blakley's method is based on geometry to share the secret. More clearly secret key is a point in a t-dimensional space which is the intersection point of the all hyperplanes. Affine hyperplanes represent n shares. Blakley scheme can be represented as a linear system $AX \mod p = T$. The general full rank matrix A is the important data in this method [29].

2.5. Ramp Secret Sharing Schemes

Another family of SSS is the **ramp SSS**. In this scheme, first a secret s is split into multiple shares $y_1, y_2, \ldots, y_N$. Then, only authorized subsets of the pieces can recover s. The encoding rule is as follows. Each secret s corresponds a set of possible share vectors:

$$Y = (y_1, y_2, \ldots, y_N).$$

Ramp SSS have a stability between coding efficiency and security. For example, in the (K, N, m)-threshold ramp SSS, we can reconstruct s from randomly K or more pieces, but no information on s can be obtained from $K - N$ or fewer pieces . Moreover, any $K - \ell$ pieces can recover s for $\ell = 1, 2, ..., N - 1$. If $N = 1$, then this (K, N, m)-threshold SSS means the usual (K, m)- ramp SSS. If a ramp SSS does not recover any part of a secret from any randomly chosen $K - \ell$ shares (for $\ell = 1, 2, ..., N$), then this scheme is called a **strong** ramp secret sharing scheme .

A linear ramp SSS is called t**-privacy** if the set of size t has no information about the secret, but a set of size at least $t + 1$ has some information about it.

3. Multisecret-Sharing Schemes Based on Linear Codes

3.1. Scheme Description

In this part, we propose a new system to construct the multisecret-sharing schemes based on linear codes. We use Blakley's method to explain our approach.

We need an $[n, k]-$ code C over $\mathbb{F}_q$ with generator matrix G.

3.1.1. Secret Distribution

Let $\mathbb{F}_q^n$ be the secret space and let a given codeword be the secret $S = (s_1, s_2, \cdots, s_n)$. The rows of a generator matrix G are minimal access elements, and all of elements of C are participants in this scheme. The dealer, knowing the secret S, computes the share y of the user with attached codeword c, by taking the scalar product of that codeword with the secret. Thus,

$$y = \langle c, s \rangle = c.S^T,$$

where ^{T} denotes transposition.

3.1.2. Secret Recovery

Consider again the system with private secret S and the coalition corresponding to the rows of G. By the preceding paragraph, we have

$$G.S^T = Y^T,$$

where $Y = (y_1, y_2, \cdots, y_k)$, and y_i is the share attached to the row i of G. The set of solutions of this system forms an affine space with associated vector space $C^\perp$. In other words, if S is a special solution then $S + d$ with $d \in C^\perp$, is also a solution and every solution is of that form. Since we assume that C is LCD or, in other words, that $C \cap C^\perp = \{0\}$, we see that the system admits a unique solution in C. Moreover, C is LCD if $\begin{pmatrix} G \\ H \end{pmatrix}$ is invertible [30]. Note that the condition that $S \in C$ can be expressed matricially as $HS^T = 0$. The secret can then be computed in practice by solving the following linear system of n equations and n unknowns.

$$\begin{aligned} G.S^T &= Y^T, \\ H.S^T &= 0. \end{aligned}$$

Note that the LCD condition implies that the matrix of this system in S, namely the square matrix $\begin{pmatrix} G \\ H \end{pmatrix}$, is of full rank n. This gives another proof of unicity of S, by inversion of $\begin{pmatrix} G \\ H \end{pmatrix}$.

The following properties of the scheme are immediate but important.

Theorem 1. *We obtain the following information in this multisecret-sharing scheme.*

1. *The access structure forms the k-tuple of codewords that are linearly independent.*
2. *The number of elements recovering the secret is at least k.*

Proof. 1. The secret is reconstructed by a full rank matrix G in which the set of rows is the said k-tuple.

2. The number of rows of G cannot be less than k by definition. So only k elements can be reached the secret, but no set of elements of size less than k can.

□

Corollary 1. *This new scheme is also a (k, n, q^k) ramp SSS with $k - 1$ privacy.*

Proof. The number of participants recovering the secret is k and the number of participants who are all of elements of C is q^k. The k-tuples of codewords of participants that are linearly independent can be reached the secret together. But some k-tuples, (those that are linearly dependent) cannot. Moreover, the secret S is split into multiple shares $(s_1, s_2, \cdots, s_n)$. □

3.2. Statistics on Coalitions

Theorem 2. *Let C be an $[n,k]$- code over $\mathbb{F}_q$ with generator matrix G. In a multisecret-sharing scheme based on C, the number of minimal coalitions is*

$$\frac{q^k(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}{k!}.$$

Proof. A minimal coalition is a set of participants, whose attached codewords form a basis of C. The number of bases of $\mathbb{F}_q$- vector space of dimension k is given by the said formula. □

Remark 1. *Note that this number is strictly less than $\binom{q^k}{k}$.*

Example 1. *We consider an LCD $[7,4]$-code C over $\mathbb{F}_2$ found by a random search in Magma [31]. A generator matrix G can be given as follows:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix}.$$

The parity-check matrix H of this code is

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}.$$

There are $2^4 = 16$ codewords in the code C . These codewords are
$\{(0000000), (1000110), (1100001), (0100111),$
$(0110000), (1110110), (1010001), (0010111),$
$(0011001), (1011111), (1111000), (0111110),$
$(0101001), (1101111), (1001000), (0001110)\}.$

Now, we examine a multisecret-sharing scheme based on C. Let the secret vector be $S = (1101111)$. We calculate the shares as follows.

$$y_1^T = g_1 S^T = \langle (1000110), (1101111) \rangle = 1$$

$$\begin{aligned} y_2^T &= g_2 S^T = \langle (0100111), (1101111) \rangle = 0 \\ y_3^T &= g_3 S^T = \langle (0010111), (1101111) \rangle = 1 \\ y_4^T &= g_4 S^T = \langle (0001110), (1101111) \rangle = 1. \end{aligned}$$

Moreover,

$$\begin{aligned} h_1 S^T &= \langle (1111100), (1101111) \rangle = 0 \\ h_2 S^T &= \langle (1111010), (1101111) \rangle = 0 \\ h_3 S^T &= \langle (0110001), (1101111) \rangle = 0. \end{aligned}$$

Therefore, we should solve the following linear system to recover the secret.

$$\begin{pmatrix} G \\ H \end{pmatrix} S^T = \begin{pmatrix} Y^T \\ 0 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Conversely, it can be seen that the secret is $S = (1100101)$ by solving the above linear system.

Example 2. *We consider an LCD $[3,2]$-code C over $\mathbb{F}_2$. Its generator matrix G and parity-check matrix H are*

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix},$$

$$H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} h_1 \end{pmatrix}.$$

It is clear that the number of codewords of C is $2^2 = 4$. These are

$$C = \{(000), (110), (101), (011)\}.$$

We try to construct a multisecret-sharing scheme based on C. Let the secret vector be $S = (011)$. We calculate the shares as follows.

$$y_1^T = g_1 S^T = \langle (110), (011) \rangle = 1$$
$$y_2^T = g_2 S^T = \langle (101), (011) \rangle = 1.$$

Moreover,

$$h_1 S^T = \langle (111), (011) \rangle = 0.$$

If we solve the following linear system, then we reach the secret.

$$\begin{pmatrix} G \\ H \end{pmatrix} S^T = \begin{pmatrix} Y^T \\ 0 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

It is seen that the secret is $S = (011)$.

Example 3. *We consider an LCD $[7,2]-$ code over $\mathbb{F}_2$, in which the generator matrix G and parity-check matrix H are given by*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix},$$

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \end{pmatrix}.$$

C has $2^2 = 4$ codewords:

$$C = \{(0000000), (1011100), (0101011), (1110111)\}.$$

We examine a multisecret-sharing scheme based on C. Let the secret vector be $S = (0101011)$. *We calculate the shares as follows.*

$$y_1^T = g_1 S^T = \langle (1011100), (0101011) \rangle = 1$$
$$y_2^T = g_2 S^T = \langle (0101011), (0101011) \rangle = 0.$$

Moreover,

$$h_1 S^T = \langle (1010000), (0101011) \rangle = 0$$
$$h_2 S^T = \langle (1101000), (0101011) \rangle = 0$$
$$h_3 S^T = \langle (1000100), (0101011) \rangle = 0$$
$$h_4 S^T = \langle (0100010), (0101011) \rangle = 0$$
$$h_2 S^T = \langle (0100001), (0101011) \rangle = 0.$$

Now, we need to solve the following linear system to obtain the secret.

$$\begin{pmatrix} G \\ H \end{pmatrix} S^T = \begin{pmatrix} Y^T \\ 0 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

By solving this system it can be seen that the secret is $S = (0101011)$.

3.3. Security Analysis

Assume that t users with $t < k$ with corresponding t codewords being linearly independent collude together to try to guess the secret. Let V_t be the span of these t codewords. They can find a complementary subspace W_t of V_t into C so that $C = V_t \oplus W_t$. Thus, the dimensions of V_t and W_t are t and $k - t$, respectively. By using Theorem 2 twice, double counting shows that the number of times any basis of V_t can be extended into a basis of C is equal to

$$X(k,t) = \frac{\prod_{i=0}^{k-1}(q^k - q^i)}{(k-t)! \prod_{i=0}^{t-1}(q^t - q^i)}.$$

Given a basis of W_t, there are q^{n-t} choices for shares of the codewords of this basis.

The probability of success of such an attack is thus

$$q^{-(k-t)} \frac{1}{X(k,t)}.$$

For instance, if $k = t + 1$, we see that, for large k, the quantity $X(k,t)$ is of the order of q^k. Thus, the security of the system requires k to be large. Having a large q is also beneficial to security but might be costly in term of arithmetic implementation.

3.4. Information Theoretic Efficiency

The **information rate** ρ of the scheme is one of the other basic parameters in secret sharing [32]. It is the ratio of the size (in q-digits) of the secret to the maximum size of the pieces given to the participants. Since the secret is a codeword of a code of dimension k, its size is k. If we regard a share as the ordered pair of a scalar y_i and a codeword, then we see that the size is $k+1$. Thus, the information rate of the SSS is

$$\rho = \frac{k}{k+1}.$$

If the information rate of a SSS is equal to one, which is the maximum possible value, then this scheme is called to be **ideal**. So the information rate of our scheme is close to one for $k \to \infty$.

4. Comparison with Other Schemes

In this section, we compare our scheme with other code based SSS by means of, respectively, the number of participants, the size of a secret, and the number of coalitions for an $[n,k]-$ code over $\mathbb{F}_q$. We denote by A, B, and C these three quantities in the following table. In the fourth column, the symbol t denotes the error-correcting capacity of code.

It transpires that the length of the code does not enter directly into the parameters of the new scheme. For codes of similar alphabets and dimensions, the new scheme allows exponentially more participants and more coalitions, compared to the other schemes, for a secret size of the same order of magnitude.

Moreover, Massey's scheme is a single secret sharing system in contrast with the other three schemes. All the schemes in Table 1 are ideal in the sense that the size of each secret equals the size of any shares. In Ding's scheme, the reconstruction algorithm is based on linear algebra, while the one in Çalkavur et al.'s scheme is based on decoding. We used Blakley's method to explain the reconstruction algorithm and obtain a linear equation system for our scheme. The advantage of our new system is the fact that it has a unique solution since it consists of n independent equations and n unknowns. So, the secret will be recovered definitely.

Table 1. Comparison with Other Schemes

System	[25]	[26]	[13]	This paper
A	$n-1$	n	n	q^k
B	q	q^k	q^k	q^n
C	$\binom{n}{k}$	$\binom{n}{k}$	$\geq \binom{n}{d-t}$	$\frac{\prod_{i=0}^{k-1}(q^k-q^i)}{k!}$
ρ	1	$\frac{k}{k-1}$	1	$\frac{k}{k+1}$

In addition, our scheme is also a (k, n, q^k) ramp SSS. It is clear that this scheme does not get out any part of a secret from any randomly chosen $k-\ell$ shares (for $\ell = 1, 2, \cdots, n$). Otherwise, this contradicts that the rows of generator matrix are linear independent. So, this new scheme is a strong ramp secret sharing scheme.

5. Conclusions and Open Problems

In this paper, we presented a new multisecret-sharing scheme based on LCD codes.

We used Blakley's method to explain the reconstruction algorithm. We determined the access structure and have calculated the information rate of this scheme. Regarding security, we can say that this system stands well for codes of a reasonably high dimension. Compared to other SSS, which are based on codes, it displays for codes of the same order of a magnitude of parameters, more users, and more coalitions at the price of shorter secret sizes.

Surprisingly, our scheme does not use the error correcting properties of the LCD codes employed. It would be nice to use them for cheater detection, for instance.

Author Contributions: Investigation: A.A. (Adel Alahmadi), A.A. (Alaa Altassan), A.A. (Ahmad AlKenani), H.S. and P.S., supervision: S.Ç.

Funding: This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. (19-130-35-RG).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. Blakley, G.R. Safeguarding Cryptographic Keys. In Proceedings of the 1979 National Computer Conference, New York, NY, USA, 4–7 June 1979; pp. 313–317.
3. Tso, R. A Study on Secret Sharing Schemes with Dishonest Dealers and Participants. Master's Thesis, University of Tsukba, Tsukuba, Japan, 2004.
4. Csirmaz, L.; Tardos, G. On-Line Secret Sharing. In Proceedings of the 13th International Conference on Information and Communication Security (ICICS 2011), Beijing, China, 23–26 November 2011. Cryptology ePrint Archive, Report 2011/174.
5. Al Ebri, N.; Yeun, C.Y. Study on Secret Sharing Schemes (SSS) and Their Applications. In Proceedings of the 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, UAE, 11–14 December 2011; pp. 40–45.
6. Martin, K. Challenging the Adversary Model in Secret Sharing Schemes. In *Coding and Cryptography II. Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts* ; Information Security Group: London, UK, 2008; pp. 45–63.
7. Iftere, S. *Secret Sharing Schemes with Applications in Security Protocols*; Technical Report TR 07-01; University Alexandruloan Cuza of Iasi, Faculty of Computer Science: Iași, Romania, 2007.
8. Horn, L. Comment: Multistage secret sharing based on one-way function. *Electron. Lett.* **1995**, *31*, 262. [CrossRef]
9. He, J.; Dawson, E. Multistage secret sharing based on one-way function. *Electron. Lett.* **1994**, *30*, 1591–1592. [CrossRef]
10. Li, H.-X.; Cheng, C.-T.; Pang, L.-J. A New (t, n)- Threshold Multisecret Sharing Scheme. In *International Conference on Computational and Information Science*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3802, pp. 421–426.
11. Pang, L.J.; Wong, Y.-M. A New (t, n)- multisecret sharing scheme based on Shamir's secret sharing. *Appl. Math.* **2005**, *167*, 840–848.
12. Yang, C.-C.; Chang, T.-Y.; Hwang, M.-S. A New $(t, n)-$ multisecret-sharing scheme. *Appl. Math. Comput.* **2004**, *151*, 483–490.
13. Çalkavur, S.; Solé, P. Multisecret sharing schemes and bounded distance decoding of linear codes. *Int. J. Comput.* **2017**, *94*, 107–114. [CrossRef]
14. Li, B. A Reliable $(k, n)-$ Image Secret Sharing Scheme. In Proceedings of the 2nd International Symposium on Dependable, Autonomic and Secure Computing DASC' 06, Indianapolis, IN, USA, 29 September–1 October 2006, pp. 1–6.
15. Massey, J.L. Linear codes with complementary duals. *Discret. Math.* **1992**, *106–107*, 337–342. [CrossRef]
16. Massey, J.L. Reversible codes. *Inf. Control* **1994**, *7*, 369–380. [CrossRef]
17. Carlet, C.; Guilley, S. Complementary dual codes for counter-measures to side-channel attacks. In Proceedings of the 4th ICMCTA Meeting, Palmela, Portugal, 15–18 September 2014.
18. Dougherty, S.T.; Kim, J.-L.; Özkaya, B.; Sok, L.; Solé, P. The combinatorics of LCD codes: Linear programming bound and orthogonal matrices. *IJICoT* **2017**, *4*, 116–128. [CrossRef]
19. Güneri, C.; Özkaya, B.; Solé, P. Quasi-cyclic complementary dual codes. *Finite Fields Appl.* **2016**, *42*, 67–80. [CrossRef]
20. Yang, X.; Massey, J.L. The condition for a cyclic code to have a complementary dual. *Discret. Math.* **1994**, *126*, 391–393. [CrossRef]

21. Sendrier, N. Linear codes with complementary duals meet the Gilbert-Varshamov bound. *Discret. Math.* **2004**, *285*, 345–347. [CrossRef]
22. Esmaeili, M.; Yari, S. On complementary-dual quasi-cyclic codes. *Finite Fields Their Appl.* **2009**, *3*, 375–386. [CrossRef]
23. Muttoo, S.K.; Lal, S. A reversible code over $GF(q)$. *Kybernetika* **1986**, *22*, 85–91.
24. Tzeng, K.K.; Hartmann, C.R.P. On the minimum distance of certain reversible cyclic codes. *IEEE Trans. Inf. Theory* **1970**, *16*, 644–646. [CrossRef]
25. 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; pp. 276–279.
26. Ding, C.; Laihonen, T.; Renvall, A. Linear Multisecret-Sharing Schemes and Error Correcting Codes. *J. Comput. Sci.* **1997**, *3*, 1023–1036.
27. Beimel, A.; Chee, Y.M.; Gwo, I.; Ling, S.; Shao, F.; Tang, Y.; Wang, H.; Xing, C. (Eds.) *Secret Sharing Schemes: A Study*; Springer: New York City, NY, USA, 2011; Volume 6639, pp. 11–46.
28. Bozkurt, I.N.; Kaya, K.; Selçuk, A.A.; Güloğlu, A.M. Threshold Cryptography Based on Blakley Secret Sharing. In Proceedings of the Information Security and Cryptology 2008, Ankara, Turkey, 25–27 December 2008.
29. Shamsoshoara, A. Overview of Blakley's Secret Sharing Scheme. *arXiv* **2019**, arXiv:1901.02802.
30. Ngo, X.T.; Bhasin, S.; Danger, J.L.; Guilley, S.; Najm, Z. Linear Complementary Dual Code Improvement to Strengthen Encoded Circuit Against Hardware Trojan Horses. In Proceedings of the 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 5–7 May 2015. [CrossRef]
31. Magma Computational Algebra System. Available online: http://magma.maths.usyd.edu.au/magma (accessed on 2 December 2019).
32. Padro, C. Robust vector space secret sharing schemes. *Inf. Process. Lett.* **1998**, *68*, 107–111. [CrossRef]