Numerical Evaluation of Algebraic Cryptography

Ravindra Babu Gudapati [1], Dr. Rajeev Jha [2], [3]

[1] *Research Scholar, Department of Mathematics, Asian International University, Ghari, Imphal West, Manipur, India.* ravi.jntv@gmail.com

[2] *Research Supervisor, Professor, Asian International University, Ghari, Imphal West, Manipur*

Abstract: *Introduction: A secret sharing scheme is a mechanism to divide up shares of a secret among numerous participants such that authorised groups of participants may piece it together but banned groups remain in the dark.*
Aim of the study: the main aim of the study is Algebraic Cryptography: Its Significance and Issues
Material and method: In this study, only black and white covert pictures are discussed. Although there exist visual cryptographic paradigms that deal with colour pictures and grayscale images, such circumstances are not considered in this study.
Conclusion: We have proposed a construction and analysis of a t-(k, n) -VCS for monochrome pictures, where t participants are crucial in a (k, n)-VCS, based on a linear algebraic method.

1. INTRODUCTION

1.1 Overview

A secret sharing scheme is a mechanism to divide up shares of a secret among numerous participants such that authorised groups of participants may piece it together but banned groups remain in the dark. In 1979, Shamir and Blakeley both separately devised a secret sharing method. In the present world, when the globe is becoming more and more digitalized every day, the idea of secret sharing is crucial. The early innovations made by the pioneers of cryptography were simple but beautiful. Imagine that a company has a computer that has certain financial information. Let's further suppose that the corporation employs n different analysts. The company now determines that any t (or more) analysts may access the data, but any t 1 (or less) analysts cannot. To make it feasible, the business may establish a password for the computer (let's say a number), then encode this secret password into n shares (let's say another number), and then distribute the shares among the individuals. Now, this must be done with extreme caution. The secret password must first be revealed when "combining" any t number of shares, and it must also remain a secret even if someone manages to get t 1 or less shares. Two stages make up a (t, n)-threshold cryptography scheme:

1. Sharing Phase: The dealer D divulges the secret to the n players at this phase. During this stage, the dealer delivers each player some information, referred to as a share.
2. Reconstruction Phase: In this stage, a group of participants (with a minimum size of t) combine their shares in order to piece together the secret.

Both Blakeley and Shamir's approaches ensure that any t out of n shares may be utilised to discover the secret. Shamir's method is predicated on the notion that each collection of t-points lying on the polynomial may be fitted with a single polynomial of degree (t 1). For instance, two points are required to accurately describe a cubic curve, three points to define a quadratic, and so on. More broadly, we need t points to uniquely identify a degree-one polynomial (t 1). The secret must be the constant term in a polynomial of degree at most t 1 in order to implement Shamir's approach, and the other coefficients of higher degree terms must be randomly selected from a suitable finite field with more than n elements. On the curve, the following n spots must be picked. On the curve, each analyst receives one point. There is just enough data to fit a t 1 degree polynomial to the points when at least t out of the n analysts divulge their points, with the constant term serving as the secret password. The key to Blakeley's technique is that any n nonparallel (n 1)-dimensional hyperplanes cross at a certain location. A unique kind of secret sharing where the secret

is a picture is called visual cryptography. We solely deal with black and white photos in this study. Although there is literature on colour and grayscale image-based visual cryptography, we are not interested in it for our study. An approach of encoding a secret picture, which is made up of a group of black and white pixels, into n shadow images known as shares, with each person in P receiving one share, is known as a visual cryptography scheme (VCS) for a set P of n participants. By duplicating their shares onto transparencies and stacking them, some qualifying subsets of P may visually retrieve the secret picture, but no banned group of participants is aware of the secret image. Naor and Shamir introduced the cryptography paradigm.

The uniqueness of visual cryptography resides in the ability of the encrypted communication to be immediately decoded by the human visual system without the use of sophisticated calculation or a computer. This is the main cause for visual cryptography's widespread interest since its debut, and consequently, much study has been done in this field. Researchers have examined several facets of VCS. Definitions have been altered to suit the requirements of various applications. Later, an alternative calculation model was put out that produces a reconstructed hidden picture of higher quality but necessitates the use of an electrical device. The most common kind of VCS handles the case when the qualifying subsets of participants (that should be able to reconstruct the secret) are merely hand-selected subsets of the set of participants P. The general access structure of this kind of visual cryptographic method is referred to as VCS. The situation where any "qualified" set X of participants is a subset of P, i.e., $X \subseteq P$, such that the cardinality of X is at least k, is handled by one instance, known as a (k, n)-threshold VCS. In this scenario, any qualifying subset of k or more participants may visually retrieve the secret picture, however prohibited sets of participants composed of k -1 people or less are unable to get any knowledge of the secret image.

1.2 Model for Black and White Visual Cryptography

In this study, only black and white covert pictures are discussed. Although there exist visual cryptographic paradigms that deal with colour pictures and grayscale images, such circumstances are not considered in this study. In this part, we go through several visual cryptography models (in terms of the underlying mathematical procedures). In this study, we consider the case when the secret recovery is flawless, or when the shared photos are piled together and the secret image is retrieved with probability 1. The deterministic model of visual cryptography is what it is known as. Only deterministic models of visual cryptography are discussed here.

1.2.1 Model for OR-Based Monochrome Deterministic VCS

It was Naor and Shamir who first developed visual cryptography in 1994. This new paradigm for cryptography can decode hidden pictures without using any cryptographic processing. Visual cryptography is tied to the human visual system, as the name indicates. Human eyes do the decryption when the qualifying shares are stacked one on top of the other. This enables anybody to use the system without needing to make any calculations or have any prior understanding of cryptography. This distinguishes visual cryptography from other well-liked conditionally safe cryptographic systems as a key benefit. This system is very safe and simple to use. Direct sharing of an electronic secret is possible, or the secret may be revealed by printing it out onto transparencies and superimposing it. The idea of a VCS for black-and-white images—which consists of a collection of black-and-white pixels—was taken into consideration by Naor and Shamir. The secret image's pixels are individually encrypted. Let's look at the scenario when the secret picture just has a single black or white pixel to better comprehend the encoding procedure. This pixel occurs after encoding in the n shares that were given to the participants.

1.2.2 Model for XOR-Based Monochrome Deterministic VCS

The poor clarity of the reconstructed picture is a drawback for OR-based visual cryptography systems. This is a flaw in the OR-based VCS that is intrinsic. There is a limit to how far it can be enhanced. With the Boolean "XOR" operation serving as the fundamental mathematical operation, Tuyls et al. provided a VCS based on the polarisation of light. A liquid crystal layer is inserted into a liquid crystal display (LCD) to polarise light. There are two benefits. The liquid crystal layer of an LCD may first be driven. Second, a workable updating mechanism is made feasible by the voltage provided to the liquid crystal layer, which enables rotation of the polarisation of light entering the layer across a certain angle. Therefore, in an XOR-based VCS, a party only has to carry one specific trusted device with a display, in contrast to OR-based systems where a participant must carry several transcripts to update the shares. Shares, or liquid crystal layers, must be put together in order to extract the hidden picture. Furthermore, these gadgets are

becoming more affordable as a result of the fast growth of technology. In any light-weight cryptographic scenario, it is fair to foresee the use of polarization-based optical cryptographic techniques.

2. LITERATURE REVIEW

Zajac, Pavol (2023) In this study, we review the literature on Multiple Right-Hand Sides (MRHS) equation-based algebraic cryptanalysis (MRHS cryptanalysis). A formal inclusion known as the MRHS equation has linear combinations of variables on the left and a set of possible values for these combinations on the right. We provide a thorough description of MRHS equation systems, including the development of this form. Then, we provide a general review of the approaches available for solving MRHS equation systems. In our last section, we investigate the use of MRHS equation systems to algebraic cryptanalysis and review prior experimental findings.

Roman'kov, Vitaly (2020) We briefly go through linear decomposition and nonlinear decomposition attacks that, in many algebraic cryptography schemes, retrieve the private shared keys from the public data using polynomial-time deterministic algorithms. Contrary to popular belief, we demonstrate that in this situation, traditional computational security assumptions are not highly significant to the security of the schemes; that is, the assumptions may be violated without also solving the algorithmic issues that they are founded on. Additionally, we provide another strategy that, in some ways, is comparable to that used by Tsaban et al. We cryptanalyze two brand-new cryptographic algorithms that have never been studied before showing how these two techniques may be applied to two well-known noncommutative protocols. Additionally, we provide a cutting-edge technique for building systems that are resistant to assaults using linear algebra. The well-known Diffie-Hellman-type (DH) and Anshel-Anshel-Goldfeld (AAG) algebraic cryptographic key-exchange protocols are proposed as upgraded variants.

Roman'kov, Vitaly (2018) In this article, we present two common algebraic cryptography systems. We demonstrate that several systems and protocols taken into consideration in the literature that use two-sided multiplications are particular instances of the first generic scheme. The second broad scheme, which connects systems and protocols based on automorphisms or endomorphisms of algebraic systems, is introduced in a manner similar to the first. We also go through some algebraic cryptanalysis uses for the membership search issue. We demonstrate how the underlined membership search problem's efficient decidability for the platform-selected algebraic system may be used to expose flaws in both strategies. Our methods of attack are based on linear or nonlinear decomposition, which complement one another. We provide a few instances of protocols and systems from the literature that use one of the two newly presented techniques in conjunction with their cryptanalysis. These protocols mostly mimic traditional algebraic cryptographic systems like Diffie-Hellman, Massey-Omura, and ElGamal. Additionally, we demonstrate that it is often possible to undermine the schemes without resolving the algorithmic issues that underlie the assumptions.

Grigoriev, Dima & Kojevnikov (2009) On noncommutative algebra, very few known cryptographic primitives are based. Due to the fact that noncommutative structures are resistant to a wide range of common cryptographic assaults, any new method is of great importance. However, the security of a cryptographic primitive cannot be relied upon due to structural complexity assumptions since cryptography does not provide security guarantees. Investigating less-stout security concepts is crucial. This work proposes new constructs of group invariant-based cryptographic primitives as well as novel approaches to their practical reinforcement. In addition, the idea of a proven break—a less secure variant of the standard cryptographic break—is proposed. In the updated version, the message's proper decryption should be supported by evidence.

Galbraith, Steven & Menezes, Alfred (2005) Public-key cryptography systems make heavy use of algebraic curves over finite fields. This article examines a few areas in algebraic curve cryptography with a focus on recent advancements in methods for the discrete logarithm problems of elliptic and hyperelliptic curves as well as computational issues in pairing-based encryption.

3. OR BASED VISUAL CRYPTOGRAPHY

In this chapter, we examine a (k, n)* -VCS, a significant class of access structures described in. It is a linear algebraic construction of the basis matrices to realise visual cryptographic schemes. The situation when one member is "essential" is covered. Generally speaking, in this case, a secret black-and-white picture is distributed among n participants in such a manner that the following two requirements are met when the secret image is recreated using the shares:

- One person is crucial in that the secret picture can only be retrieved with his attendance. In other words, without him present, it is impossible to restore the hidden picture.
- To retrieve the hidden picture, it must include the shares of at least k participants, including the crucial participant.

3.1 Construction and Analysis of Some Efficient t-(k, n) $*$ - VCS

Let the group of participants, P, be defined as 1, 2, 3,..., n. Let 0 t k n be three numbers, where t indicates the minimum number of participants needed to recover the secret picture and k indicates the minimum number of people needed to recover the secret image. Let's suppose that the first t participants, or 1, 2,..., t, are the key players to maintain generality. Other than 0≤ t ≤ k ≤ n, we have not as of yet imposed any restrictions on the parameters t, k, and n. It's important to note that we are only interested in parameter triplets (t, k, n) that allow for a useful visual cryptographic method. For instance, if t = k, then n can only take on the relevant value of k, as if n > k, then the remaining nk participants are optional and may be disregarded while keeping the secret a secret. Again, all participants are necessary if k equals n, t equals k equals n, or t equals n, in which case the resultant scheme is once again a (n, n)-VCS. The original (k, n)-threshold VCS, in which any k or more participants may retrieve the secret, exists when t = 0 and n k > 1. In this situation, no participant is necessary. From this point on, a triplet of the form (t, k, n) is always a meaningful triplet. It should also be emphasised that if (t, k, n) is a meaningful triplet, then (t-1, k-1, n-1) is as well. We will now go through how to create the basis matrices needed to realise a t-(k, n)* -VCS. The procedure is simple and effective in that it just calls for the solution of a set of linear equations in order to create the basis matrices. This technique is a development of the linear algebraic approach first presented by Adhikari et al. in and later expanded in.

3.1.1 Construction of a t-(k, n) $*$ -VCS: Linear Algebraic Technique

We assign the variable xi to each participant i for all i = 1, 2,..., n. If |X| = k and X is a minimum qualifying set for a t-(k, n) -VCS, then we need to have each of the following: 1, 2,... t ∈ X and |X| = k therefore has in total $\binom{n-t}{k-t}$ these subsets. We organise the subsets in the following manner based on the lexicographic ordering: B1, B2, . . . , Br where r= $\binom{n-t}{k-t}$. For example, if P = {1, 2, 3, . . . , 6}, t = 2 and k = 4 then B1 = {1, 2, 3, 4}, B2 = {1, 2, 3, 5}, B3 = {1, 2, 3, 6}, B4 = {1, 2, 4, 5}, B5 = {1, 2, 4, 6} and B6 = {1, 2, 5, 6}.

With the exception of the final subset Br if r is odd, let's couple the successive subsets to create $\lfloor \frac{r}{2} \rfloor$ groups. Only one set, Br itself, will be present in the final group for odd r. As a result, for every r, we have $\lfloor \frac{r}{2} \rfloor$ many groups.

The groups for 2-(4, 6)$*$ -VCS are as follows:

Group 1: (B1, B2); Group 2: (B3, B4); and Group 3: (B5, B6).

In general, the i-th group can be described as follows:

$$i\text{th Group} = \begin{cases} (B_{2i-1}, B_{2i}), & \text{for } 1 \le i \le \lceil \frac{r-2}{2} \rceil, \text{ and any } n > 2; \\ (B_{r-1}, B_r), & \text{for even } r > 2 \text{ and } i = \frac{r}{2}; \\ (B_r), & \text{for odd } r > 2 \text{ and } i = \lceil \frac{r}{2} \rceil. \end{cases}$$

Let us denote by fBj = 0, the linear equation $\sum_{k \in B_j} x_k$ = 0 and by fBj = 1, the linear equation $\sum_{k \in B_j} x_k$ =1.

We consider the following linear equation systems over the binary field Z2:

For 1 ≤ i ≤ $\lceil \frac{r-2}{2} \rceil$ and for any r ≥ 3,

$$\left.\begin{matrix} f_{B_{2i-1}} = 0 \\ f_{B_{2i}} = 0 \end{matrix}\right\} \cdots (i) \quad \text{and} \quad \left.\begin{matrix} f_{B_{2i-1}} = 1 \\ f_{B_{2i}} = 1 \end{matrix}\right\} \cdots (i')$$

For i = $\frac{r}{2}$ and for even r > 3,

$$\left.\begin{matrix} f_{B_{r-1}} = 0 \\ f_{B_r} = 0 \end{matrix}\right\} \cdots (\frac{r}{2}) \quad \text{and} \quad \left.\begin{matrix} f_{B_{r-1}} = 1 \\ f_{B_r} = 1 \end{matrix}\right\} \cdots (\frac{r'}{2})$$

For i = $\lceil \frac{r}{2} \rceil$ and for odd r ≥ 3,

$$\left.\begin{matrix} f_{B_r} = 0 \end{matrix}\right\} \cdots (\lceil \frac{r}{2} \rceil) \quad \text{and} \quad \left.\begin{matrix} f_{B_r} = 1 \end{matrix}\right\} \cdots (\lceil \frac{r'}{2} \rceil)$$

Let for any r ≥ 3 and 1 ≤ i ≤ $\lceil \frac{r-2}{2} \rceil$, S_i^0 and S_i^1 denote the Boolean matrices whose columns are all possible solutions of the equations (i) and (i 0) respectively. Similarly, for any even (odd) r ≥ 3, $S^0_{\frac{r}{2}}$ $(S^0_{\lceil \frac{r}{2} \rceil})$ and $S^1_{\lceil \frac{r}{2} \rceil}$ $(S^1_{\lceil \frac{r}{2} \rceil})$ denote the Boolean matrices corresponding the solutions of the equations $(\frac{r}{2})$ $((\lceil \frac{r}{2} \rceil))$ and $(\frac{r'}{2})$ $(\lceil \frac{r'}{2} \rceil)$ respectively.

Result 3.1: The way we have constructed S0 and S1 it is now easy to see that each block S^1_i can be obtained from S_i^0 by adding a particular solution of the system (i 0) to each column of S_i^0

Theorem 3.1 The pair of matrices (S0 , S1) obtained by the above algorithm, constitute basis matrices of the t-(k, n) ∗ -VCS.

4. XOR BASED NON-MONOTONE T-(K, N) ∗ -VISUAL CRYPTOGRAPHIC SCHEMES USING LINEAR ALGEBRA

The Boolean operation "OR" is the mathematical operation that underlies the actual physical execution of the systems outlined. However, the biggest issues with any OR-based visual cryptography system are the very low contrast and large share size (pixel expansion). The Boolean "XOR" operation served as the foundation for the VCS developed by Tuyls et al., which was based on the polarisation of light. They also built an XOR-based (n, n)-VCS and demonstrated that an XOR-based (2, n)-VCS is comparable to a binary code. Additional study was conducted, and numerous publications were published. One for more research, maybe. All of these papers have the trait of being non-monotone, which means that even if they stack their shares, the superset of the smallest qualified set won't be able to learn the secret. For broad access structures, the authors in provided a step-by-step building approach to produce and distribute shares of a visual secret. The participants must carry numerous shares, one for each minimum qualified set, and they must be aware of the precise minimal qualified set that wishes to extract the secret in advance since the participants' construction does not use basis matrices. By using basis matrices to represent the complete scenario, we are able to solve these issues.

We generalise the idea of an XOR-based non-monotonic (k, n)-threshold access structure to an XOR-based non-monotonic (k, n)-threshold access structure where any (k - t) participant, including t-essential players, may expose the secret. The access structure is often public knowledge for most practical cases, which is the rationale for the non-monotonicity. In other words, the participants are fully aware of the eligible sets anda prohibited sets. As a result, every minimally qualified subset of a qualified set of participants may provide the matching shares to reconstruct the secret picture. Since all minimum qualified sets that correspond to the access structure are collected, this restriction is adequate. We develop a novel XOR-based VCS for the nonmonotone t-(k, n)-threshold access structure based on

this insight. This structure is a generalisation of the non-monotonic (k, n)-threshold access structure in that it results if we set t = 0.

4.1 The Model and Construction for t-(k, n) ∗ -NM-XVCS

All along, we use standardised symbols and notations. We go through some of the fundamental notations and techniques required for this chapter in order to be thorough. We wish to emphasise that we work with all of the significant triplets (t, k, and n). For instance, discussing a t-(n, n)* -VCS based on XOR does not make much sense if k = n. Henceforth, we only consider meaningful triplets (t, k, n). The case t = 0 with n ≥ k > 1 is the XOR based (k, n)-threshold VCS where no participant is essential and any k of them can recover the secret. In this chapter, we consider Q = Qmin = {X ⊂ P : 1, 2, . . . , t ∈ X and |X| = k}, the collection of all minimal qualified sets of participants. The collection of forbidden sets is denoted by F, where Y ∈ F if and only if there exists i ∈ {1, 2, . . . , t} such that i /∈ Y or |Y | ≤ k − 1. Note that in this chapter, we do not care about any subset Y ∈ 2^P such that X ⊂ Y, for some X ∈ Qmin. This makes the access structure non-monotone.

Example 4.1 If P = {1, 2, 3, 4, 5, 6}, t = 2 and k = 4 then Qmin consists of the following minimal qualified subsets of participants B1 = {1, 2, 3, 4}, B2 = {1, 2, 3, 5}, B3 = {1, 2, 3, 6}, B4 = {1, 2, 4, 5}, B5 = {1, 2, 4, 6}, B6 = {1, 2, 5, 6}. Note that {1, 2, 3} and {2, 3, 4, 5, 6} are some of the members of F.

Notations: Let S be an n × m Boolean matrix and let X ⊂ P. By S[X] we denote the matrix obtained by restricting the rows of S to the indices belonging to X. Further, for any X ⊂ P the vector that resulted from doing a boolean XOR operation "+", to the rows of S[X] is denoted by SX. The Hamming weight of the row vector which represents the number of ones in the vector SX is denoted by w(SX).

We are now in a position to give definition of a t-(k, n) ∗ -NM-XVCS and then the definition of the basis matrices realizing it.

Definition 4.1 Let P = {1, 2, 3, . . . , n} be a set of participants among which the first t participants are essential. A t-(k, n) ∗ -NM-XVCS on P is a visual cryptographic system that meets the two requirements below:

1. Any group of participants with the very minimum of qualifications may learn the secret.
2. No prohibited group of participants is aware of the identity of the secret picture.

Definition 4.2.2 (via Collection of Matrices) Let P = {1, 2, 3, . . . , n} be a set of participants. Let (Qmin, F) be the access structure defined on P. Let m and {hX}X∈Qmin be non-negative integers satisfying 1 ≤ hX ≤ m. Two collections of n × m binary matrices C0 and C1 realizes (Qmin, F)-NM-XVCS , if there exists {αX > 0 : X ∈ Qmin} such that

1. For any S ∈ C0, the "XOR" operation of the rows of S[X] for any minimal qualified set X results in a vector v0 satisfying w(v0) ≤ hX − αX · m.
2. For any T ∈ C1, the "XOR" operation of the rows of T[X] for any minimal qualified set X results in a vector v1 satisfying w(v1) ≥ hX.
3. Any forbidden set Y ∈ F has no information on the shared image. Formally, the two collections of |Y | × m matrices Dt , with t ∈ {0, 1}, produced by limiting each of the n m matrices in Ct to the rows indexed by Y are identical in that they both include the same matrices with the same frequencies.

Definition 4.2.3 (via Basis Matrices) A t-(k, n) ∗ -NM-XVCS If two sets of non-negative real numbers XXXQmin and tXXXQmin exist and the following two criteria true, is realised using two n m binary matrices called basis matrices.

1. (contrast condition) If X ∈ Qmin, then S_X^0 the "XOR" of the rows indexed by X of S^0, satisfies $w(S_X^0)$ ≤ tX − αX · m; whereas, for S 1 it results in $w(S_X^1)$ ≥ tX.
2. (security condition) If Y = {i1, i2, . . . , is} ∈ F then the two s × m matrices S^0 [Y] and S^1 [Y] obtained by restricting S^0 and S^1 respectively to rows i1, i2, . . . , is are identical up to a column permutation.

The pixel expansion of the scheme is denoted by the number m. Additionally, X and X m stand for the relative contrast and contrast of the recovered picture created by the minimum qualified set X, respectively. We will now go through

an effective technique for creating the basis matrices for a t-(k, n) - NM-XVCS. We continue to use the notations mentioned above..

4.1.1 The Construction

We associate a Boolean variable xi to each participant i for all i = 1, 2, . . . , n. If X ∈ Qmin then X must contain 1, 2, . . . , t and |X| = k. Thus |Qmin| = $\binom{n-t}{k-t}$ We arrange the elements of Qmin in lexicographic order, say B1, B2, . . . , Br, where r= $\binom{n-t}{k-t}$ We now pair the consecutive subsets, except for the last subset Br if r is odd, to form $\lfloor \frac{r}{2} \rfloor$ groups. For odd r, the last group consists of only one set, Br itself. Hence for any r, we have $\lfloor \frac{r}{2} \rfloor$ many groups.

The groups for 2-(4, 6)$_*$ -NM-XVCS as in Example 5.2.1 are as follows:

Group 1: (B1, B2); Group 2: (B3, B4); Group 3: (B5, B6).

In general, the i-th group can be described as follows:

$$i\text{th Group} = \begin{cases} (B_{2i-1}, B_{2i}), & \text{for } 1 \le i \le \lceil \frac{r-2}{2} \rceil, \text{ and any } n > 2; \\ (B_{r-1}, B_r), & \text{for even } r > 2 \text{ and } i = \frac{r}{2}; \\ (B_r), & \text{for odd } r > 2 \text{ and } i = \lceil \frac{r}{2} \rceil. \end{cases}$$

Let fBj = 0 and fBj = 1 respectively denote the linear equations $\sum_{k \in B_j} x_k$ = 0 and $\sum_{k \in B_j} x_k$ = 1.

For i = 1, 2, . . . , r, let Ci = {i1, i2, . . . , iti }, where

$$C_i = \begin{cases} \mathcal{P} \setminus (B_{2i-1} \cup B_{2i}), & \text{for } 1 \le i \le \lceil \frac{r-2}{2} \rceil, \text{ and any } n > 2; \\ \mathcal{P} \setminus (B_{r-1} \cup B_r), & \text{for even } r > 2 \text{ and } i = \frac{r}{2}; \\ \mathcal{P} \setminus B_r, & \text{for odd } r > 2 \text{ and } i = \lceil \frac{r}{2} \rceil. \end{cases}$$

Be aware that for certain i, Ci could be empty. Let FCi = 0 represent the system of linear equations that looks like this:

$$x_{i_1} = 0, \; x_{i_2} = 0, \ldots, \; x_{i_{t_i}} = 0.$$

We take into account the following sets of linear equations over the field Z2:

For $1 \le i \le \lceil \frac{r-2}{2} \rceil$ and for any r ≥ 3,

$$\left.\begin{aligned} f_{B_{2i-1}} &= 0 \\ f_{B_{2i}} &= 0 \\ \mathcal{F}_{C_i} &= 0 \end{aligned}\right\} \cdots (i) \quad \text{and} \quad \left.\begin{aligned} f_{B_{2i-1}} &= 1 \\ f_{B_{2i}} &= 1 \\ \mathcal{F}_{C_i} &= 0 \end{aligned}\right\} \cdots (i')$$

For i = $\frac{r}{2}$ and for even r > 3,

$$\left.\begin{array}{ll} f_{B_{r-1}} & =0 \\ f_{B_r} & =0 \\ \mathcal{F}_{C_i} & =0 \end{array}\right\} \cdots\left(\frac{r}{2}\right) \quad \text{and} \quad \left.\begin{array}{ll} f_{B_{r-1}} & =1 \\ f_{B_r} & =1 \\ \mathcal{F}_{C_i} & =0 \end{array}\right\} \cdots\left(\frac{r'}{2}\right)$$

For i = $\lceil \frac{r}{2} \rceil$ and for odd r ≥ 3,

$$\left.\begin{array}{ll} f_{B_r} & =0 \\ \mathcal{F}_{C_i} & =0 \end{array}\right\} \cdots\left(\lceil \frac{r}{2} \rceil\right) \quad \text{and} \quad \left.\begin{array}{ll} f_{B_r} & =1 \\ \mathcal{F}_{C_i} & =0 \end{array}\right\} \cdots\left(\lceil \frac{r'}{2} \rceil\right)$$

Let for any r ≥ 3 and 1 ≤ i ≤ $\lceil \frac{r-2}{2} \rceil$, S_i^0 denote the Boolean matrix whose columns are all possible solutions of the system (i). Also, let S_i^1 indicate the Boolean matrix (i 0) whose columns represent all conceivable system solutions. The same goes for any even (odd) r ≥ 3, $S_{\frac{r}{2}}^0 \ (S_{\lceil \frac{r}{2} \rceil}^0)$ and $S_{\lceil \frac{r}{2} \rceil}^1 \ (S_{\lceil \frac{r}{2} \rceil}^1)$ denote the Boolean matrices corresponding to the systems $(\frac{r}{2}) \ ((\lceil \frac{r}{2} \rceil))$ and $(\frac{r'}{2}) \ (\lceil \frac{r'}{2} \rceil)$ respectively.

Let (S0 , S1) indicate the two Boolean matrices that were created by concatenating them.:

$$S^0 = S_1^0 || S_2^0 || \cdots || S_{\lceil \frac{r}{2} \rceil}^0 \text{ and } S^1 = S_1^1 || S_2^1 || \cdots || S_{\lceil \frac{r}{2} \rceil}^1.$$

5. CONCLUSION

We have proposed a construction and analysis of a t-(k, n) -VCS for monochrome pictures, where t participants are crucial in a (k, n)-VCS, based on a linear algebraic method. To create systems of linear equations that we could solve to create the initial basis matrices, we grouped the minimum qualifying sets, two at a time. Then, in order to lessen the pixel expansion, we used the method of eliminating the common columns found in the original basis matrices. In order to quickly calculate the basis matrices necessary to implement the XOR-based scheme, we have proposed a (Black and White) XOR-based model of the (k, n)- VCS with multiple key players. We have also provided a construction approach based on tools from linear algebra. The XOR-based model's contrast is 2k times greater than that of the current OR-based approaches. We demonstrated that for certain limited access architectures, pixel expansion and contrast optimality have been attained.

6. REFERENCES

[1] Zajac, Pavol. (2023). Algebraic Cryptanalysis with MRHS Equations. Cryptography. 7. 19. 10.3390/ cryptography7020019.

[2] Roman'kov, Vitaly. (2020). Algebraic cryptanalysis and new security enhancements. Moscow Journal of Combinatorics and Number Theory. 9. 123-146. 10.2140/moscow.2020.9.123.

[3] Roman'kov, Vitaly. (2018). Two general schemes of algebraic cryptography. Groups Complexity Cryptology. 10. 10.1515/gcc-2018-0009.

[4] Grigoriev, Dima & Kojevnikov, Arist & Nikolenko, Sergey. (2009). Algebraic cryptography: New constructions and their security against provable break. St. Petersburg Mathematical Journal, v.20, 937-953 (2009). 20. 10.1090/S1061-0022-09-01079-6.

[5] Galbraith, Steven & Menezes, Alfred. (2005). Algebraic curves and cryptography. Finite Fields and Their Applications. 11. 544-577. 10.1016/j.ffa.2005.05.001.

[6] Adhikari, A., “Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images”, Designs, Codes and Cryptography, Springer Journal, DOI 10.1007/s10623-013-9832-5.

[7] Adhikari, A., Dutta, T. K. and Roy, B., “A New Black and White Visual Cryptographic Scheme for General Access Structures,” Indocrypt’04, Lecture Notes in Computer Science, Springer-Verlag, 3348, 399-413 (2004).
[8] Blundo, C., D’arco, P., Santis, A. De and Stinson, D. R., “Contrast optimal threshold visual cryptography”, SIAM J. of Discrete Math., Vol. 16, issue 2, 224-261 (2003).
[9] Bose, M. and Mukerjee, R, “Optimal (k, n) visual cryptographic schemes for general k”, Designs, Codes and Cryptography, 55(1), 19-35 (2010).
[10] Chang, C-C., Lin, C.-C. and Tu, H.N., “Safeguarding visual information using (t, n) verifiable secret shares”, Journal of Computers 22 (2) (2011).

DOI: https://doi.org/10.15379/ijmst.v10i4.2390