Result Computation for University of Ibadan Statistics Department Using Anonymous Threshold Scheme

O. A. Otekunrin
Department of Statistics
University of Ibadan, Nigeria
+234-803-835-7957
oa.alawode@mail.ui.edu.ng

P. A. Emehinola
Department of Statistics
University of Ibadan, Nigeria
+234-706-635- 4730
emehinolapatience@gmail.com

ABSTRACT
In this paper, we constructed (2, 7)-anonymous threshold scheme from the (49, 56, 8, 7, 1) Resolvable Balanced Incomplete Block Design (RBIBD) using MATLAB codes. The (2, 7)-anonymous threshold scheme was then applied to Result Processing Scheme in the Department of Statistics, University of Ibadan. The scheme developed satisfied the security requirements of authenticity, integrity and verifiability thus making it better than the scheme currently being used in the Department.

CCS Concepts
• **Security and privacy → Security privacy → Access control**

Keywords
Secret sharing; Resolvable Balanced Incomplete Block Designs; Anonymous threshold scheme

1. INTRODUCTION
Keeping secrets is as old as man. In the early times, human beings kept secrets by inscribing special writings on rocks and walls, keeping of special articles in earthen wares and burying underground etcetera. This has changed drastically today where secrets are kept today using advanced forms of computer technology. Most of our personal information are now on the databases of government, banks, healthcare institutions and other organisations. When these secrets are properly managed, our lives, businesses, political activities and so on are ultimately protected. Secure key management has been an active area of research since the independent works of [1] and [2].

2. SECRET SHARING SCHEMES
Secret sharing is a method of dividing a secret K among a set of $P = \{P_1, P_2, \dots, P_n\}$ of n participants. Each of the participants is given a part (*share)* of the secret in such a way that only certain specified (qualified) subsets of the n participants can reconstruct the secret by combining their shares while certain set of participants gets no information about the secret even when they combine their shares[3].

Variants of secret sharing schemes abound in literature. These include the works of [4], [5], [6], [7], [8], [9], [10] among others. Some applications of secret sharing schemes, which include private proximity testing and recursive information hiding, can be found in [11] and [12].

2.1 Perfect (t, w)-Threshold Scheme
A perfect (t, w)threshold scheme is defined by [13] as follows: Suppose that t and w are integers such that $2 \leq t \leq w$. A perfect (t, w)-threshold scheme is a method of sharing a secret value K among a finite set $P = \{P_1, \dots, P_w\}$ of w participants in such a way that any t participants can compute the value of K but no group of $t - 1$ (or fewer) participants can compute any information about the value of K from the information they hold collectively.

2.2 Anonymous Threshold Schemes
Anonymous threshold schemes were first investigated by [14]. In an anonymous threshold scheme, the secret can be reconstructed without knowledge of which participants hold which shares. The computation of the secret can be carried out by giving the shares to a black box that does not know the identities of the participants holding those shares, [15]. According to [16], the scheme can be used to provide access to a secure area because security is provided without any need for a separate identification protocol.

Ideal anonymous secret sharing schemes were investigated by [17]. In this scheme, the size of the shares given to each participant is equal to the size of the secret. They also proved that an ideal anonymous (t, w)-threshold scheme can be realized if and only if $t = 1 \text{ or } n$. The $(2, w)$-threshold scheme was characterized by [18] in terms of a regular difference family while [19] constructed anonymous secret sharing schemes using combinatorial designs.

2.2.1 Definition: [13]
A perfect (*t*, *w*)-threshold scheme is an *anonymous threshold scheme* if the following two properties are satisfied:
1. the *w* participants receive *w* distinct shares,
2. the secret can be computed solely as a function of *t* shares, without the knowledge of which participant holds which share.

CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria.

3. BALANCED INCOMPLETE BLOCK DESIGNS (BIBD)

3.1 Definition: [3]

Let v, b, r, w, λ be positive integers such that $v > w \geq 2$. A (v, b, r, w, λ) BIBD is a pair (X, A) such that:

- X is a set of v elements called points
- A is a collection of subsets of X called block
- Each block contains exactly w points
- Every pair of distinct points is contained in exactly λ blocks

3.2 Resolvable Balanced Incomplete Block Design (RBIBD)

3.2.1 Definition: [13]

Suppose (X, A) is a (v, b, r, w, λ)-BIBD. A parallel class in (X, A) is a subset of disjoint blocks from A whose union is X. A partition of A into r parallel classes is called a resolution, and (X, A) is said to be a resolvable BIBD if A has at least one resolution. In an RBIBD, each point occurs exactly one block in each part of the partition (or parallel class)

3.2.2 Necessary Conditions for the Existence of an RBIBD: [20]

- $\lambda(v-1) \equiv 0(mod(k-1))$
- $v \equiv 0\ (mod\ k)$

An example of a resolvable BIBD is the $(9, 12, 4, 3, 1)$RBIBD displayed in Table 1. Each column is a parallel class.

Table 1: (9, 12, 4, 3, 1) RBIBD

{1, 2, 3}	**{1, 4, 7}**	**{1, 5, 9}**	**{1, 6, 8}**
{4, 5, 6}	**{2, 5, 8}**	**{2, 6, 7}**	**{2, 4, 9}**
{7, 8, 9}	**{3, 6, 9}**	**{3, 4, 8}**	**{3, 5, 7}**

4. OVERVIEW OF RESULT COMPUTATION PROCESS IN STATISTICS DEPARTMENT, UNIVERSITY OF IBADAN

Result computation issues are highly sensitive matters in any University setting. In the Department of Statistics, University of Ibadan, result computation issues are handled through the collaborative efforts of eight out of the total population of staff members of the Department. They are the Head of Department (HOD), the Examination Officer, four Undergraduate Level Advisers and two System Analysts. The HOD is the overall Coordinator of result computation matters in the Department. The Level Advisers coordinate students' registration while the Examination Officer coordinates undergraduate students' examinations and receives examination results from course lecturers. The two System Analysts ensure that the students' registration details and results are correctly stored on the system. The program used for computing the results was developed by a trusted computer programmer who is not a member of the University community. The HOD, Examination Officer, the final year level adviser and the two system analysts were all trained to handle the program. Each of them is assumed to be trustworthy and each has individual password that give them access to the program. There is also a wireless intranet provision that allows these five members to connect their personal laptops to the main computer system and the result computation can only be done in the office where the main computer system is located. Any of these five members can therefore access the program and compute results, once he/she gains access to the Office.

5. CONSTRUCTION OF (*2, W*) - ANONYMOUS THRESHOLD SCHEME FROM (v, b, r, w, 1)-RBIBD

The following illustration, from [13] showed that $(v, b, r, w, 1)$-RBIBD can be used to construct anonymous (*2, w*)-threshold schemes.

Suppose that (X, A) is a $(v, b, r, w, 1)RBIBD$, then there are $r = \frac{v-1}{w-1}$ parallel classes, $\pi_1, \pi_2, \ldots, \pi_r$, in the RBIBD. The Dealer D chooses a secret value K from a specified set of secrets $\mathcal{K} = (1, 2, .., r)$. This implies that there are r possible secrets to choose from. The Dealer shares the secret value K among the set $P = (P_1, P_2, \ldots, P_w)$ of w participants with the assumption that $D \notin P$. To share the secret K, D gives some partial information, called a share, from a specified share set S, to each of the participants. The share set S has cardinality v. (X, A) and its resolution are known to all the w participants.

To share secret K, $1 \leq K \leq r$, D chooses a random block $A \in \pi_K$ and gives the w points in A to the w participants, each of the w participants receiving one point.

Assume that any two participants with shares q and f want to obtain the secret, recall that (X, A) is a BIBD with $\lambda = 1$, then there is a unique block A such that $(q, f) \subseteq A$. Thus, the two shares can be used to find the parallel class π_K that contains A and the secret is revealed as K.

The scheme is anonymous because the computation of the secret depends on the shares and not on the identities of the shareholders. The security of the scheme is guaranteed because any one share cannot lead to the determination of the secret key to the program. Also, the authenticity, integrity and verifiability requirements for the scheme are satisfied since any two participants must submit their shares to the machine in order to have access to the program.

6. THE RESULT PROCESSING SCHEME

$(49, 56, 8, 7, 1)RBIBD$ was selected from a list of RBIBDs in [21] because of its suitability to the application area. An algorithm with five cell executions was written in MATLAB to generate the parallel classes for $(49, 56, 8, 7, 1)RBIB$. The steps taken in the generation of the parallel classes are illustrated with the aid of the workflow chart in Figure 1 while the parallel classes for the RBIBD are displayed in Table 2.

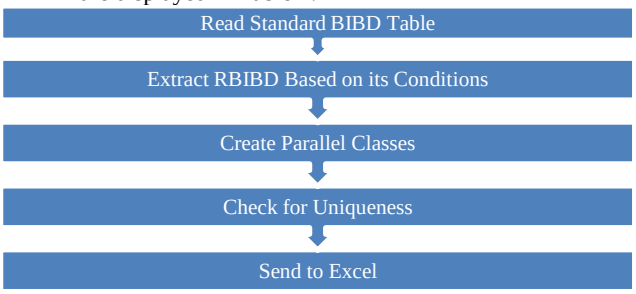

Figure 1: Workflow chart for the construction of the Parallel Classes for (49, 56, 8, 7, 1) RBIBD

Table 2: Parallel Classes for (49, 56, 8, 7, 1) RBIBD

π_1	π_2
43 17 33 35 11 22 9	5 14 23 47 37 43 34
31 30 34 2 45 29 8	17 8 45 42 9 10 12
36 15 3 14 49 20 38	28 13 18 24 31 1 3
42 13 7 47 28 23 16	22 27 49 4 30 35 39
24 37 44 10 19 1 6	25 20 2 21 6 15 16

48	18	5	21	46	40	41
25	27	26	39	32	4	12

36	41	29	44	38	32	33
26	46	48	40	19	11	7

π_3

46	44	29	30	12	3	33
35	8	1	41	36	25	47
23	21	42	34	32	31	15
14	11	43	22	48	6	49
38	45	9	28	27	20	5
13	17	24	2	18	19	26
10	40	39	37	4	16	7

π_4

36	44	40	11	39	10	22
26	14	37	24	30	20	47
9	13	12	27	42	31	1
4	48	28	43	5	6	2
35	25	49	7	19	23	45
18	46	33	8	17	3	29
38	34	32	21	41	16	15

π_5

33	42	27	1	8	24	3
43	41	10	21	30	26	46
31	22	47	34	32	7	35
9	19	17	39	28	25	6
44	5	18	11	37	23	14
40	15	48	12	29	2	36
16	13	20	45	38	4	49

π_6

34	22	39	45	46	1	27
38	48	15	33	44	5	41
9	42	4	16	25	19	13
29	14	17	23	7	20	40
12	47	8	32	31	37	43
11	2	6	26	36	49	24
28	3	21	10	18	30	35

π_7

11	2	45	35	39	31	24
23	22	5	8	32	44	27
21	18	49	20	33	30	3
17	25	19	34	14	26	40
38	1	6	46	43	29	47
16	36	10	48	13	37	9
12	28	15	4	41	7	42

π_8

13	28	6	29	35	26	22
42	44	14	11	16	36	23
9	15	4	27	49	18	12
17	24	48	2	47	21	10
32	20	37	31	19	41	30
5	34	33	46	38	1	40
25	39	7	8	3	43	45

The $(49, 56, 8, 7, 1)$RBIBD has point set $X = \{1, 2, 3, \ldots, 49\}$

The $b = 56$ blocks are arranged into $r = \frac{v-1}{w-1} = \frac{49-1}{7-1} = 8$ parallel classes, denoted by $\boldsymbol{\pi_1, \pi_2, \ldots, \pi_8}$, as shown in Table 1 above.

Suppose a trusted Dealer D chooses a secret value K from a specified set of secrets $\mathcal{K} = (1, 2, .., 8)$. This implies that there are 8 possible secrets to choose from. D shares the secret value K among the set $P = (P_1, P_2, \ldots, P_7)$ of $w = 7$ participants with the assumption that $D \notin P$. The share set S has cardinality $v = 49$. The $(49, 56, 8, 7, 1)$RBIBD and its resolution are known to the 7 participants. In sharing the secret K, $1 \leq K \leq r$, D chooses a random block $A \in \pi_K$ and gives the $w = 7$ points in A to the 7 participants, each of the 7 participants receiving one point.

Assume that any 2 of the 7 participants with shares q and f want to obtain the secret, recall that this RBIBD has its $\lambda = 1$, then there is a unique block A such that $(q, f) \subseteq A$. Thus, the parallel class π_K that contains A is determined and the secret is revealed as K.

The (2,7)-anonymous threshold scheme described above is applied as follows:

Assume that a seven (7) member committee, $P_1, \ldots P_7$, coordinates result-related issues for students in the Department. The committee comprises of the Head of Department (1), the Examination Officer (1), the Level Advisors (4) and the System Analyst (1). Assume that a trusted dealer D, a third party outside the Department, wrote the computer program that computes students' results. To prevent unauthorized access to the program, he devised a $(2,7)$ Anonymous Scheme that allows at least any two of the seven member committee access to the program. D shares the secret key among the 7 committee members such that each member receives a distinct share and the identity of each shareholder is not linked to their respective shares. To reconstruct the secret, any two members submit their shares to the machine, the shares are kept secret by the machine, the secret key is obtained and access is thus provided to the two members.

For example, if D wants to share the secret key 8 among the 7 participants, D picks a random block in π_8, (say $\{29, 11, 27, 2, 31, 46, 8\}$). These are distributed to members of the committee in such a way that each member is not linked to their respective shares. Any two of the shares e.g. 27 and 2 can be used to reveal the secret. This is because the unique block containing 27 and 2 is $\{29, 11, 27, 2, 31, 46, 8\}$ and the parallel class that contains this block is π_8. So, the secret is 8.

Since any one member cannot access the program to compute the students' results, the scheme ensures that the security requirements of authenticity, integrity and verifiability for the scheme are satisfied. Thus, the scheme is preferable to the one being used in the Department.

7. CONCLUSION

Secret sharing schemes are used for increasing the security of important information. Different secret sharing schemes abound in literature one of which is Anonymous threshold scheme. In this paper, the (2,7) anonymous threshold scheme was constructed from the (49, 56, 8, 7, 1) RBIBD. The (2, 7) anonymous threshold scheme was then applied to Result Processing System in the Department of Statistics, University of Ibadan. The scheme developed satisfied the security requirements of authenticity, integrity and verifiability since a single participant cannot have access to the program used for computing the students' result. This makes the scheme better than the one currently being used in the Department.

8. REFERENCES

[1] Shamir, A. 1979. How to share a secret. *Communication of ACM*, 22 (11), 612-613.

[2] Blakley, G. R. 1979. Safeguarding cryptographic keys, In *AFIPS Conference Proceedings* 48, 313- 317.

[3] Adhikari, A. 2013. *Design Theory and Visual Cryptographic Schemes.* Department of Pure Mathematics, University of Calcutta, Kolkata. Available Online at: www.imbic.org/avishek.html.

[4] Mustafa U., Rifat, Y., Vasif V. N. and Guzin U. 2008. *(2,2)*-Secret Sharing Scheme with Improved Share Randomness. *IEEE, 978-1-4244-2881-6/08,* 1-5.

[5] Jun, A. and Guisheng L. 2006. A Novel Non-interactive Verifiable Secret Sharing Scheme. In *Proceedings of Chunbo Ma, Communication Technology, ICCT'06, International Conference* (27-30 November, 2006) 1-4.

[6] Feng, J. ,Wu, H., Tsai, C., Chang, Y.and Chu,Y. 2008. Visual Secret Sharing For Multiple Secrets. *Pattern Recognition* 41, 3572 – 3581.

[7] Weir J. and Yan, W. 2009. Sharing Multiple Secrets Using Visual Cryptography. *IEEE 978-1-4244-3828-0/09,* 509-512.

[8] Shao, J. and Cao, Z. 2005. A new efficient (t, n) Verifiable Multi-Secret Sharing (VMSS) based on YCH Scheme. *Applied Mathematics and Computation* 168 (1), 135–140.

[9] Harn, L. and Lin, C. 2010. Strong (n, t, n) verifiable secret sharing scheme. *Information Sciences* 180, 3059–3064.

[10] Binu, V.P, Nair, D. G., and Sreekumar A. 2016. Secret Sharing Homomorphism and Secure E-voting. Available Online at: https://arxiv.org/pdf/1602.05372

[11] Narayanan, A., Thiagarajan, N., Lakhani, M.Hamburg, M. and Boneh, D. 2009. *Optimistic Fair Exchange with Multiple Arbiters*. Brown University, Providence, RI, USA. Available Online at: https://eprint.iacr.org/2009/069.pdf

[12] Katta, S. 2010. *Recursive Information Hiding in Visual Cryptography.* Department of Computer Science,

Oklahoma State University, Stillwater. OK 74078. Available Online at: https://arxiv.org/pdf/1004.4914

[13] Stinson, D. R. 2004. *Combinatorial Designs: Constructions and Analysis.* Springer-Verlag New York, Inc.

[14] Stinson, D. R. and Vanstone, S. A. 1988. A combinatorial approach to threshold schemes. *SIAM Journal of Discrete Mathematics* 1(2), 230–236.

[15] Blundo, C. and Stinson, D. R. 1996. *Anonymous Secret Sharing Schemes.* Available Online at: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.47.9460&rep=rep1...pdf

[16] Kishimoto, W., Okada, K., Kurosawa, K. and Ogata, W. 2002. On the Bound for Anonymous Secret Sharing Schemes. *Discrete Applied Mathematics* 121, 193–202.

[17] Phillips, S. J. and Phillips, N. C. 1992. Strongly Ideal Secret Sharing Schemes. *Journal of Cryptology*, 5, 185–191.

[18] Miao, Y. 2003. A combinatorial characterization of regular anonymous perfect threshold schemes. *Information Processing Letters* 85, 131–135.

[19] Deng, Y., Guo, L. and Liu, M. 2007. Constructions for Anonymous Secret Sharing Schemes Using Combinatorial Designs. *Acta Mathematicae Applicatae Sinica, English Series* 23, 67-78.

[20] Abel, R. J. R, Ge, G. and Yin, J. 2007. Resolvable and Near- Resolvable Designs. In *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., Boca Raton: CRC Press, 124 – 132.

[21] Mathon, R. and Rosa, A. 2007. 2-(v, k, λ) Designs of Small Order. In *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., Boca Raton: CRC Press, 25- 58.