RESULT PROCESSING SCHEME FOR UNIVERSITY OF IBADAN STATISTICS DEPARTMENT USING ANONYMOUS THRESHOLD SCHEME

Oluwaseun A. Otekunrin

Department of Statistics, Faculty of Science, University of Ibadan, Nigeria

Corresponding author: Oluwaseun A. Otekunrin, oa.alawode@mail.ui.edu.ng

ABSTRACT: Secret sharing schemes are used for increasing the security of important information. A type of secret sharing schemes is the anonymous threshold scheme. In this paper, the (2, 7) anonymous threshold scheme for result processing scheme in the Department of Statistics, University of Ibadan, Nigeria was proposed. The (49, 56, 8, 7, 1) Resolvable Balanced Incomplete Block Designs (RBIBD) was selected from a standard list of RBIBDs. The parallel classes for the RBIBD were constructed using a successive diagonalizing algorithm. The (2, 7) anonymous threshold scheme was developed using the parallel classes of the selected RBIBD. The threshold scheme was then applied to Result Processing Scheme in the Department of Statistics, University of Ibadan. The scheme developed satisfied the security and integrity requirements since a single participant cannot access the program used for computing the students' result. This makes it better than the one currently in use in the Department.

***KEYWORDS*:** Secret Sharing; Resolvable Balanced Incomplete Block Designs; Successive Diagonalization; Participants; Parallel Classes; Access control.

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 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 ([Sha79]) and ([Bla79]).

2. SECRET SHARING SCHEMES

Secret sharing is a method of dividing a secret k among a set of $P=\{P_1, P_2,..., P_n\}$ of n participants. Each of the participants is given a part (*share)* of the secret in such a way that only certain qualified subsets of the n participants can reconstruct the secret by combining their shares while certain set of participants get no information about the secret even when their shares are combined ([Adh13]).

Variants of secret sharing schemes abound in literature. These include the works of ([M+08, JG06, F+08, WY09, SC05, HL10, BNS16]) among others.

Some applications of secret sharing schemes, which include missile launching and opening a bank vault, can be found in ([BS96]) and ([K+02]). In this paper, the (2, 7) anonymous threshold scheme was applied to result processing scheme in the Department of Statistics, University of Ibadan, Nigeria.

Definition 1 ([Sti04]):

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 $P=\{P_1,..., P_w\}$ 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.

Definition 2 ([SV88]):

The threshold scheme is an **anonymous threshold scheme** if 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 the shares ([BS96]).

Ideal anonymous secret sharing schemes, a type of anonymous threshold schemes, were investigated by ([PP92]). 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 $t=1$ *or* n. The $(2,w)$-threshold scheme was characterized by ([Mia03]) in terms of a regular difference family while ([DGL07]) constructed anonymous secret sharing schemes using combinatorial designs.

Definition 3 ([Sti04]):

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.

3. BALANCED INCOMPLETE BLOCK DESIGNS (BIBD)

Balanced Incomplete Block Designs are binary, proper and equi-replicated designs that possess optimal properties with various applications.

Definition 4 ([MR07]):

Let v, b, r, w, λ be positive integers such that $v>w\geq 2$. A **Balanced Incomplete Block Design** (BIBD) is a pair (V, B) where V is a v-set and B is a collection of b w-subsets of V (blocks) such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. The integers v, b, r, w, and λ are the parameters of the BIBD.

Definition 5 ([Sti04]): Resolvable Balanced Incomplete Block Design (RBIBD)

Suppose (V, B) is a (v, b, r, k, λ) BIBD. A **parallel class** in (V, B) is a subset of disjoint blocks from B whose union is V. A partition of B into r parallel classes is called a **resolution**, and (V, B) is said to be a **Resolvable BIBD** if B has at least one resolution. The necessary conditions for the existence of an RBIBD can be found in ([AGY07])

The b blocks are grouped into sets with each group containing each treatment once. This is of great advantage in experiments where it is feasible to run and analyze the design replicate by replicate or omit some replicates ([CR00])

Theorem 1: ([Sti04])

Suppose there is a resolvable $(v, b, r, w, 1)$-BIBD. Then there exists an anonymous perfect $(2, w)$-threshold scheme with $|S| = v$ and $|K| = r = (v - 1)/(w - 1)$. S is the share set and K is the set of r possible secrets.

4. OVERVIEW OF RESULT PROCESSING SCHEME IN STATISTICS DEPARTMENT, UNIVERSITY OF IBADAN

Result processing issues are highly sensitive matters in any University setting. In the Department of Statistics, University of Ibadan, result processing issues are handled through the collaborative efforts of the Head of Department (HOD), the Examination Officer, the Undergraduate Final Year Level Adviser and two Computer System Operators. The HOD is the overall Coordinator of all examination and examination results' matters in the Department. The Final Year Level Adviser coordinates students' registration while the Examination Officer coordinates undergraduate students' examinations and receives examination results from course lecturers. The two System Operators ensure that the students' registration details and results are correctly stored on the computer 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 are all trained to handle the program. Each of them is assumed to be trustworthy and each has individual password that give him/her 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.

5. METHODOLOGY

A *(49, 56, 8, 7, 1)RBIBD* was selected from a list of RBIBDs in ([MR07]) because of its suitability to the application area. A successive diagonalization algorithm from ([KF79]) was used to generate the parallel classes for the selected RBIBD. The parallel classes generated are displayed in Table 1

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

Π_1								Π_5						
1	2	3	4	5	6	7		1	11	21	24	34	37	47
8	9	10	11	12	13	14		2	12	15	25	35	38	48
15	16	17	18	19	20	21		3	13	16	26	29	39	49
22	23	24	25	26	27	28		4	14	17	27	30	40	43
29	30	31	32	33	34	35		5	8	18	28	31	41	44
36	37	38	39	40	41	42		6	9	19	22	32	42	45
43	44	45	46	47	48	49		7	10	20	23	33	36	46
Π_2								Π_6						
1	8	15	22	29	36	43		1	12	16	27	31	42	46
2	9	16	23	30	37	44		2	13	17	28	32	36	47
3	10	17	24	31	38	45		3	14	18	22	33	37	48
4	11	18	25	32	39	46		4	8	19	23	34	38	49
5	12	19	26	33	40	47		5	9	20	24	35	39	43
6	13	20	27	34	41	48		6	10	21	25	29	40	44
7	14	21	28	35	42	49		7	11	15	26	30	41	45
Π_3								Π_7						
1	9	17	25	33	41	49		1	13	18	23	35	40	45
2	10	18	26	34	42	43		2	14	19	24	29	41	46
3	11	19	27	35	36	44		3	8	20	25	30	42	47
4	12	20	28	29	37	45		4	9	21	26	31	36	48
5	13	21	22	30	38	46		5	10	15	27	32	37	49
6	14	15	23	31	39	47		6	11	16	28	33	38	43
7	8	16	24	32	40	48		7	12	17	22	34	39	44
Π_4								Π_8						
1	10	19	28	30	39	48		1	14	20	26	32	38	44
2	11	20	22	31	40	49		2	8	21	27	33	39	45
3	12	21	23	32	41	43		3	9	15	28	34	40	46
4	13	15	24	33	42	44		4	10	16	22	35	41	47
5	14	16	25	34	36	45		5	11	17	23	29	42	48
6	8	17	26	35	37	46		6	12	18	24	30	36	49
7	9	18	27	29	38	47		7	13	19	25	31	37	43

6. THE RESULT PROCESSING SCHEME

Suppose that a seven (7) member committee, P_1, P_2, ..., 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 Advisers (4) and the System Analyst (1). Assume that a trusted dealer *D*, a third party outside the Department, writes the computer program that computes students' results. To prevent unauthorized access to the program, he devises a *(2, 7)* Anonymous Scheme that allows 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. The (49, 56, 8, 7, 1) RBIBD has point set V = {1, 2, 3,….., 49}.

The $b=56$ blocks are arranged into $r=v-1/w-1=8$ parallel classes, denoted by $\Pi_1, \Pi_2,\ldots,\Pi_8$ as shown in Table 1 above.

Let $K= (1, 2,\ldots,r)$ be the set of secrets *D* can choose from. Suppose that *D* chooses a secret value *k* from the specified set of secrets. *D* shares the secret value *k* among the set $P = (P_1, P_2, \ldots, P_7)$ of $w=7$ participants. In sharing the secret *k*, $1\leq k\leq r$, *D* chooses a random block $B\in\Pi_k$ and gives the $w=7$ points in *B* to the *7* participants, each of the *7* participants receiving a distinct share. The identity of each shareholder is not linked to their respective shares. The share set *S* has cardinality $v=49$. The $(49,56,8,7,1)$RBIBD and its resolution are known to the 7 participants.

Assume that any 2 of the 7 participants with shares say, *18* and *49* want to have access to the program, they need to obtain the secret value *k*. The two members submit their shares to the main computer system, the shares submitted are kept secret by the system and these shares are used by the system to compute the secret value. For the computation, there is a unique block $B=(6,12,18,24,30,36,49)$ such that $(18,49)\subseteq B$ since $\lambda = 1$ for the *(49, 56, 8, 7, 1)* RBIBD. Thus, the parallel class Π_k that contains *B* is uniquely determined as Π_k and the secret is revealed as *8*.

The scheme is anonymous because the computation of the secret depends on the shares and not on the identities of the shareholders. Since any one member cannot access the program to compute the students' results, the security and integrity requirements for the scheme are satisfied. Thus, the scheme is preferable to the one currently in use in the Department.

6.1 Security Requirement Analysis

To show that the scheme is secure, suppose that a participant with share say, *12* wants to have access to the program. He submits his share to the computer system. The secret key cannot be determined because $12\in B_F$ and $B_F\in\Pi_F$ where $1\leq F\leq r$. For any value *F* of the secret, there is exactly one block $B_F\in\Pi_F$ such that $12\in B_F$ Any of the *r* possible blocks could have been used by *D* to distribute shares to the participants in *P*. Thus, any possible value for the secret is consistent for $12\in V$ and the secret cannot be uniquely obtained.

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 (49, 56, 8, 7, 1) RBIBD was selected from a standard list of RBIBDs. The parallel classes for the RBIBD were constructed using the successive diagonalizing algorithm. The (2, 7) anonymous threshold scheme was developed from the parallel classes of the selected RBIBD. 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 and integrity requirements 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.

REFERENCES

[Adh13] **A. Adhikari** - *Design Theory and Visual Cryptographic Schemes.* Department of Pure Mathematics, University of Calcutta, Kolkata, 2013. Available Online at: www.imbic.org/avishek.html.

[AGY07] **R. J. R. Abel, G. Ge, J. Yin** - *Resolvable and Near-Resolvable Designs* in Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz, Eds., Boca Raton: CRC Press, 124 – 132, 2007.

[Bla79] **G. R. Blakley** - *Safeguarding Cryptographic Keys* in Proceedings of the AFIPS Conference 48, 1979.

[BS96] **C. Blundo, D. R. Stinson** - *Anonymous Secret Sharing Schemes.* Available Online at: citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.47.9460&rep= rep1...pdf, 1996.

[BNS16] **V. P. Binu, D. G. Nair, A. Sreekumar** - *Secret Sharing Homomorphism and Secure E-voting.* Available Online at: https://arxiv.org/pdf/1602.05372, 2016.

[CR00] **D. R. Cox, N. Reid** - *The Theory of the Design of Experiments.* Chapman & Hall/CRC Boca Raton, Florida 33431, 2000.

[DGL07] **Y. Deng, L. Guo, M. Liu** - *Constructions for Anonymous Secret Sharing Schemes using Combinatorial Designs.* Acta Mathematicae Applicatae Sinica, English Series, Vol. 23: 67-78, 2007.

[F+08] **J. Feng, H. Wu, C. Tsai, Y. Chang, Y. Chu** - *Visual Secret Sharing for Multiple Secrets.* Pattern Recognition, Vol. 41: 3572 – 3581, 2008.

[HL10] **L. Harn, C. Lin** - *Strong (n, t, n) verifiable secret sharing scheme.* Information Sciences, Vol. 180: 3059 – 3064, 2010.

[JG06] **A. Jun, L. Guisheng** - *A Novel Non-interactive Verifiable Secret Sharing Scheme* in Proceedings of Chunbo Ma, Communication Technology International Conference, 2006.

[KF79] **M. Khare, W. T. Federer** - *A Simple Construction Procedure for Resolvable Incomplete Block Designs*. Biometrics Unit, Cornell University, Ithaca, New York, 1979.

[K+02] **W. Kishimoto, K. Okada, K. Kurosawa, W. Ogata** - *On the Bound for Anonymous Secret Sharing Schemes*. Discrete Applied Mathematics, Vol. 121: 193–202, 2002.

[Mia03] **Y. Miao** - *A Combinatorial Characterization of Regular Anonymous Perfect Threshold Schemes*. Information Processing Letters, Vol. 85: 131–135, 2003.

[MR07] **R. Mathon, A. Rosa** - *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, 2007.

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

[PP92] **S. J. Phillips, N. C. Phillips** - *Strongly Ideal Secret Sharing Schemes*. Journal of Cryptology, Vol. 5: 185–191, 1992.

[Sha79] **A. Shamir** - *How to share a secret*, Communication of ACM, Vol. 22, No. 11: 612-613, 1979.

[Sti04] **D. R. Stinson** - *Combinatorial Designs: Constructions and Analysis.* Springer-Verlag, New York, Inc., 2004.

[SC05] **J. Shao, Z. Cao** - *A new efficient (t, n) Verifiable Multi-Secret Sharing (VMSS) based on YCH Scheme.* Applied Mathematics and Computation, Vol. 168, No. 1: 135–140, 2005.

[SV88] **D. R. Stinson, S. A. Vanstone** - *A Combinatorial Approach to Threshold Schemes.* SIAM Journal of Discrete Mathematics, Vol.1, No. 2: 230–236, 1988.

[WY09] **J. Weir, W. Yan** - *Sharing Multiple Secrets Using Visual Cryptography.* IEEE 978-1-4244-3828-0/09, 509-512, 2009.

Tibiscus