Chapter 10

Conclusions

We have given the theoretical background of Secret Sharing Schemes and the historical development of the subject. The evolution of the various schemes are accounted in the initial chapters. We have included a few examples to improve the readability of the thesis. We have tried to maintain the rigor of the treatment of the subject.

The limitations and disadvantages of the various forms secret sharing schemes are brought out. Several new schemes for both dealing and combining are included in the thesis. We have introduced a new number system, called, POB number system. Representation using POB number system has been presented. Algorithms for finding the POB number and POB value are given. We have also proved that the representation using POB number system is unique and is more efficient. Being a new system, there

is much scope for further development in this area.

Our research findings are well appreciated by the research community in Computer Science. Appendix. 3 contains the list of publications of some of our research findings in this area.

We have improved many of the existing schemes and introduced a few new schemes. The introduction of POB number system and using it for some very efficient uniform secret sharing scheme is the most significant achievement of this research work.

All the new schemes we have introduced have the potential for a lot of research activities in future. We propose to continue this work and explore the possibilities of using POB number system in other areas also.

APPENDIX 1

The Distribution of keys

Let us return to the example we considered in section 1.3. We denote the scientists by the letters: a, $b, \ldots, k$. As per our scheme, any 6 of the 11 scientists together should be able to open the cabinet using the keys in their possession. The scheme envisages the use of at least one key from each of the six scientists. There are in all 462 different locks and keys. The keys are numbered from 0 to 461. For each lock there must be exactly six keys as no five from among the 11 scientists could be able to open a particular lock. The allotment of each key to the scientists are denoted by 1s against their names in the column. For example key no.3 will be available with scientists - e, f, g, i, j and k. In other words, any permutation of six 1s and five 0s denote allotment of a specific key. Every such permutation can be considered as a unique 11 digit binary number having a specific decimal value. We have chosen to assign the key numbers in the ascending order of its decimal value. For example, key no.0 has 63 as decimal value, where as key no.35 has 343 as its value.

An algorithm for allocating the 462 keys is given in Table 10.1.

It may be noted that the numeric value corresponding to the distribution of keys of a specific lock can be easily computed as follows:

The key no. can be computed from the corresponding binary number in the table using the following formula:

$$keyno. = \sum_{j=0}^{10} b_j \binom{j}{p_j}$$

where

$$p_j = \sum_{i=0}^{j} b_i,$$

and $b_{10}b_9 \ldots b_0$ is the binary number. For example, the key no. corresponding to the binary number

$$\begin{aligned} 10110011010 &= \binom{10}{6} + \binom{8}{5} + \binom{7}{4} + \binom{4}{3} + \binom{3}{2} + \binom{1}{1} \\ &= 210 + 56 + 35 + 4 + 3 + 1 \\ &= 309. \end{aligned}$$

It may be noted that the table consists of all binary numbers of length 11 and having precisely 6 1s, arranged in the ascending order of its decimal value.

Table 10.1: The distribution of keys of various locks to the scientists.

Sl. No.	Scientists a b c d e f g h i j k	Binary value	Sl. No.	Scientists a b c d e f g h i j k	Binary value
0	0 0 0 0 0 1 1 1 1 1 1	63	33	0 0 1 0 0 1 1 1 1 1 0	318
1	0 0 0 0 1 0 1 1 1 1 1	95	34	0 0 1 0 1 0 0 1 1 1 1	335
2	0 0 0 0 1 1 0 1 1 1 1	111	35	0 0 1 0 1 0 1 0 1 1 1	343
3	0 0 0 0 1 1 1 0 1 1 1	119	36	0 0 1 0 1 0 1 1 0 1 1	347
4	0 0 0 0 1 1 1 1 0 1 1	123	37	0 0 1 0 1 0 1 1 1 0 1	349
5	0 0 0 0 1 1 1 1 1 0 1	125	38	0 0 1 0 1 0 1 1 1 1 0	350
6	0 0 0 0 1 1 1 1 1 1 0	126	39	0 0 1 0 1 1 0 0 1 1 1	359
7	0 0 0 1 0 0 1 1 1 1 1	159	40	0 0 1 0 1 1 0 1 0 1 1	363
8	0 0 0 1 0 1 0 1 1 1 1	175	41	0 0 1 0 1 1 0 1 1 0 1	365
9	0 0 0 1 0 1 1 0 1 1 1	183	42	0 0 1 0 1 1 0 1 1 1 0	366
10	0 0 0 1 0 1 1 1 0 1 1	187	43	0 0 1 0 1 1 1 0 0 1 1	371
11	0 0 0 1 0 1 1 1 1 0 1	189	44	0 0 1 0 1 1 1 0 1 0 1	373
12	0 0 0 1 0 1 1 1 1 1 0	190	45	0 0 1 0 1 1 1 0 1 1 0	374
13	0 0 0 1 1 0 0 1 1 1 1	207	46	0 0 1 0 1 1 1 1 0 0 1	377
14	0 0 0 1 1 0 1 0 1 1 1	215	47	0 0 1 0 1 1 1 1 0 1 0	378
15	0 0 0 1 1 0 1 1 0 1 1	219	48	0 0 1 0 1 1 1 1 1 0 0	380
16	0 0 0 1 1 0 1 1 1 0 1	221	49	0 0 1 1 0 0 0 1 1 1 1	399
17	0 0 0 1 1 0 1 1 1 1 0	222	50	0 0 1 1 0 0 1 0 1 1 1	407
18	0 0 0 1 1 1 0 0 1 1 1	231	51	0 0 1 1 0 0 1 1 0 1 1	411
19	0 0 0 1 1 1 0 1 0 1 1	235	52	0 0 1 1 0 0 1 1 1 0 1	413
20	0 0 0 1 1 1 0 1 1 0 1	237	53	0 0 1 1 0 0 1 1 1 1 0	414
21	0 0 0 1 1 1 0 1 1 1 0	238	54	0 0 1 1 0 1 0 0 1 1 1	423
22	0 0 0 1 1 1 1 0 0 1 1	243	55	0 0 1 1 0 1 0 1 0 1 1	427
23	0 0 0 1 1 1 1 0 1 0 1	245	56	0 0 1 1 0 1 0 1 1 0 1	429
24	0 0 0 1 1 1 1 0 1 1 0	246	57	0 0 1 1 0 1 0 1 1 1 0	430
25	0 0 0 1 1 1 1 1 0 0 1	249	58	0 0 1 1 0 1 1 0 0 1 1	435
26	0 0 0 1 1 1 1 1 0 1 0	250	59	0 0 1 1 0 1 1 0 1 0 1	437
27	0 0 0 1 1 1 1 1 1 0 0	252	60	0 0 1 1 0 1 1 0 1 1 0	438
28	0 0 1 0 0 0 1 1 1 1 1	287	61	0 0 1 1 0 1 1 1 0 0 1	441
29	0 0 1 0 0 1 0 1 1 1 1	303	62	0 0 1 1 0 1 1 1 0 1 0	442
30	0 0 1 0 0 1 1 0 1 1 1	311	63	0 0 1 1 0 1 1 1 1 0 0	444
31	0 0 1 0 0 1 1 1 0 1 1	315	64	0 0 1 1 1 0 0 0 1 1 1	455
32	0 0 1 0 0 1 1 1 1 0 1	317	65	0 0 1 1 1 0 0 1 0 1 1	459

Table 10.1 Continues

Sl. No.	Scientists a b c d e f g h i j k	Binary value	Sl. No.	Scientists a b c d e f g h i j k	Binary value
66	0 0 1 1 1 0 0 1 1 0 1	461	99	0 1 0 0 1 1 1 0 0 1 1	627
67	0 0 1 1 1 0 0 1 1 1 0	462	100	0 1 0 0 1 1 1 0 1 0 1	629
68	0 0 1 1 1 0 1 0 0 1 1	467	101	0 1 0 0 1 1 1 0 1 1 0	630
69	0 0 1 1 1 0 1 0 1 0 1	469	102	0 1 0 0 1 1 1 1 0 0 1	633
70	0 0 1 1 1 0 1 0 1 1 0	470	103	0 1 0 0 1 1 1 1 0 1 0	634
71	0 0 1 1 1 0 1 1 0 0 1	473	104	0 1 0 0 1 1 1 1 1 0 0	636
72	0 0 1 1 1 0 1 1 0 1 0	474	105	0 1 0 1 0 0 0 1 1 1 1	655
73	0 0 1 1 1 0 1 1 1 0 0	476	106	0 1 0 1 0 0 1 0 1 1 1	663
74	0 0 1 1 1 1 0 0 0 1 1	483	107	0 1 0 1 0 0 1 1 0 1 1	667
75	0 0 1 1 1 1 0 0 1 0 1	485	108	0 1 0 1 0 0 1 1 1 0 1	669
76	0 0 1 1 1 1 0 0 1 1 0	486	109	0 1 0 1 0 0 1 1 1 1 0	670
77	0 0 1 1 1 1 0 1 0 0 1	489	110	0 1 0 1 0 1 0 0 1 1 1	679
78	0 0 1 1 1 1 0 1 0 1 0	490	111	0 1 0 1 0 1 0 1 0 1 1	683
79	0 0 1 1 1 1 0 1 1 0 0	492	112	0 1 0 1 0 1 0 1 1 0 1	685
80	0 0 1 1 1 1 1 0 0 0 1	497	113	0 1 0 1 0 1 0 1 1 1 0	686
81	0 0 1 1 1 1 1 0 0 1 0	498	114	0 1 0 1 0 1 1 0 0 1 1	691
82	0 0 1 1 1 1 1 0 1 0 0	500	115	0 1 0 1 0 1 1 0 1 0 1	693
83	0 0 1 1 1 1 1 1 0 0 0	504	116	0 1 0 1 0 1 1 0 1 1 0	694
84	0 1 0 0 0 0 1 1 1 1 1	543	117	0 1 0 1 0 1 1 1 0 0 1	697
85	0 1 0 0 0 1 0 1 1 1 1	559	118	0 1 0 1 0 1 1 1 0 1 0	698
86	0 1 0 0 0 1 1 0 1 1 1	567	119	0 1 0 1 0 1 1 1 1 0 0	700
87	0 1 0 0 0 1 1 1 0 1 1	571	120	0 1 0 1 1 0 0 0 1 1 1	711
88	0 1 0 0 0 1 1 1 1 0 1	573	121	0 1 0 1 1 0 0 1 0 1 1	715
89	0 1 0 0 0 1 1 1 1 1 0	574	122	0 1 0 1 1 0 0 1 1 0 1	717
90	0 1 0 0 1 0 0 1 1 1 1	591	123	0 1 0 1 1 0 0 1 1 1 0	718
91	0 1 0 0 1 0 1 0 1 1 1	599	124	0 1 0 1 1 0 1 0 0 1 1	723
92	0 1 0 0 1 0 1 1 0 1 1	603	125	0 1 0 1 1 0 1 0 1 0 1	725
93	0 1 0 0 1 0 1 1 1 0 1	605	126	0 1 0 1 1 0 1 0 1 1 0	726
94	0 1 0 0 1 0 1 1 1 1 0	606	127	0 1 0 1 1 0 1 1 0 0 1	729
95	0 1 0 0 1 1 0 0 1 1 1	615	128	0 1 0 1 1 0 1 1 0 1 0	730
96	0 1 0 0 1 1 0 1 0 1 1	619	129	0 1 0 1 1 0 1 1 1 0 0	732
97	0 1 0 0 1 1 0 1 1 0 1	621	130	0 1 0 1 1 1 0 0 0 1 1	739
98	0 1 0 0 1 1 0 1 1 1 0	622	131	0 1 0 1 1 1 0 0 1 0 1	741

Table 10.1 Continues

Sl. No.	Scientists a b c d e f g h i j k	Binary value	Sl. No.	Scientists a b c d e f g h i j k	Binary value
132	0 1 0 1 1 1 0 0 1 1 0	742	165	0 1 1 0 1 1 0 0 0 1 1	867
133	0 1 0 1 1 1 0 1 0 0 1	745	166	0 1 1 0 1 1 0 0 1 0 1	869
134	0 1 0 1 1 1 0 1 0 1 0	746	167	0 1 1 0 1 1 0 0 1 1 0	870
135	0 1 0 1 1 1 0 1 1 0 0	748	168	0 1 1 0 1 1 0 1 0 0 1	873
136	0 1 0 1 1 1 1 0 0 0 1	753	169	0 1 1 0 1 1 0 1 0 1 0	874
137	0 1 0 1 1 1 1 0 0 1 0	754	170	0 1 1 0 1 1 0 1 1 0 0	876
138	0 1 0 1 1 1 1 0 1 0 0	756	171	0 1 1 0 1 1 1 0 0 0 1	881
139	0 1 0 1 1 1 1 1 0 0 0	760	172	0 1 1 0 1 1 1 0 0 1 0	882
140	0 1 1 0 0 0 0 1 1 1 1	783	173	0 1 1 0 1 1 1 0 1 0 0	884
141	0 1 1 0 0 0 1 0 1 1 1	791	174	0 1 1 0 1 1 1 1 0 0 0	888
142	0 1 1 0 0 0 1 1 0 1 1	795	175	0 1 1 1 0 0 0 0 1 1 1	903
143	0 1 1 0 0 0 1 1 1 0 1	797	176	0 1 1 1 0 0 0 1 0 1 1	907
144	0 1 1 0 0 0 1 1 1 1 0	798	177	0 1 1 1 0 0 0 1 1 0 1	909
145	0 1 1 0 0 1 0 0 1 1 1	807	178	0 1 1 1 0 0 0 1 1 1 0	910
146	0 1 1 0 0 1 0 1 0 1 1	811	179	0 1 1 1 0 0 1 0 0 1 1	915
147	0 1 1 0 0 1 0 1 1 0 1	813	180	0 1 1 1 0 0 1 0 1 0 1	917
148	0 1 1 0 0 1 0 1 1 1 0	814	181	0 1 1 1 0 0 1 0 1 1 0	918
149	0 1 1 0 0 1 1 0 0 1 1	819	182	0 1 1 1 0 0 1 1 0 0 1	921
150	0 1 1 0 0 1 1 0 1 0 1	821	183	0 1 1 1 0 0 1 1 0 1 0	922
151	0 1 1 0 0 1 1 0 1 1 0	822	184	0 1 1 1 0 0 1 1 1 0 0	924
152	0 1 1 0 0 1 1 1 0 0 1	825	185	0 1 1 1 0 1 0 0 0 1 1	931
153	0 1 1 0 0 1 1 1 0 1 0	826	186	0 1 1 1 0 1 0 0 1 0 1	933
154	0 1 1 0 0 1 1 1 1 0 0	828	187	0 1 1 1 0 1 0 0 1 1 0	934
155	0 1 1 0 1 0 0 0 1 1 1	839	188	0 1 1 1 0 1 0 1 0 0 1	937
156	0 1 1 0 1 0 0 1 0 1 1	843	189	0 1 1 1 0 1 0 1 0 1 0	938
157	0 1 1 0 1 0 0 1 1 0 1	845	190	0 1 1 1 0 1 0 1 1 0 0	940
158	0 1 1 0 1 0 0 1 1 1 0	846	191	0 1 1 1 0 1 1 0 0 0 1	945
159	0 1 1 0 1 0 1 0 0 1 1	851	192	0 1 1 1 0 1 1 0 0 1 0	946
160	0 1 1 0 1 0 1 0 1 0 1	853	193	0 1 1 1 0 1 1 0 1 0 0	948
161	0 1 1 0 1 0 1 0 1 1 0	854	194	0 1 1 1 0 1 1 1 0 0 0	952
162	0 1 1 0 1 0 1 1 0 0 1	857	195	0 1 1 1 1 0 0 0 0 1 1	963
163	0 1 1 0 1 0 1 1 0 1 0	858	196	0 1 1 1 1 0 0 0 1 0 1	965
164	0 1 1 0 1 0 1 1 1 0 0	860	197	0 1 1 1 1 0 0 0 1 1 0	966

Table 10.1 Continues

Sl. No.	Scientists a	b	c	d	e	f	g	h	i	j	k	Binary value	Sl. No.	Scientists a	b	c	d	e	f	g	h	i	j	k	Binary value
199	0	1	1	1	1	0	0	1	0	1	0	970	231	1	0	0	1	0	0	0	1	1	1	1	1167
198	0	1	1	1	1	0	0	1	0	0	1	969	232	1	0	0	1	0	0	1	0	1	1	1	1175
200	0	1	1	1	1	0	0	1	1	0	0	972	233	1	0	0	1	0	0	1	1	0	1	1	1179
201	0	1	1	1	1	0	1	0	0	0	1	977	234	1	0	0	1	0	0	1	1	1	0	1	1181
202	0	1	1	1	1	0	1	0	0	1	0	978	235	1	0	0	1	0	0	1	1	1	1	0	1182
203	0	1	1	1	1	0	1	0	1	0	0	980	236	1	0	0	1	0	1	0	0	1	1	1	1191
204	0	1	1	1	1	0	1	1	0	0	0	984	237	1	0	0	1	0	1	0	1	0	1	1	1195
205	0	1	1	1	1	1	0	0	0	0	1	993	238	1	0	0	1	0	1	0	1	1	0	1	1197
206	0	1	1	1	1	1	0	0	0	1	0	994	239	1	0	0	1	0	1	0	1	1	1	0	1198
207	0	1	1	1	1	1	0	0	1	0	0	996	240	1	0	0	1	0	1	1	0	0	1	1	1203
208	0	1	1	1	1	1	0	1	0	0	0	1000	241	1	0	0	1	0	1	1	0	1	0	1	1205
209	0	1	1	1	1	1	1	0	0	0	0	1008	242	1	0	0	1	0	1	1	0	1	1	0	1206
210	1	0	0	0	0	0	1	1	1	1	1	1055	243	1	0	0	1	0	1	1	1	0	0	1	1209
211	1	0	0	0	0	1	0	1	1	1	1	1071	244	1	0	0	1	0	1	1	1	0	1	0	1210
212	1	0	0	0	0	1	1	0	1	1	1	1079	245	1	0	0	1	0	1	1	1	1	0	0	1212
213	1	0	0	0	0	1	1	1	0	1	1	1083	246	1	0	0	1	1	0	0	0	1	1	1	1223
214	1	0	0	0	0	1	1	1	1	0	1	1085	247	1	0	0	1	1	0	0	1	0	1	1	1227
215	1	0	0	0	0	1	1	1	1	1	0	1086	248	1	0	0	1	1	0	0	1	1	0	1	1229
216	1	0	0	0	1	0	0	1	1	1	1	1103	249	1	0	0	1	1	0	0	1	1	1	0	1230
217	1	0	0	0	1	0	1	0	1	1	1	1111	250	1	0	0	1	1	0	1	0	0	1	1	1235
218	1	0	0	0	1	0	1	1	0	1	1	1115	251	1	0	0	1	1	0	1	0	1	0	1	1237
219	1	0	0	0	1	0	1	1	1	0	1	1117	252	1	0	0	1	1	0	1	0	1	1	0	1238
220	1	0	0	0	1	0	1	1	1	1	0	1118	253	1	0	0	1	1	0	1	1	0	0	1	1241
221	1	0	0	0	1	1	0	0	1	1	1	1127	254	1	0	0	1	1	0	1	1	0	1	0	1242
222	1	0	0	0	1	1	0	1	0	1	1	1131	255	1	0	0	1	1	0	1	1	1	0	0	1244
223	1	0	0	0	1	1	0	1	1	0	1	1133	256	1	0	0	1	1	1	0	0	0	1	1	1251
224	1	0	0	0	1	1	0	1	1	1	0	1134	257	1	0	0	1	1	1	0	0	1	0	1	1253
225	1	0	0	0	1	1	1	0	0	1	1	1139	258	1	0	0	1	1	1	0	0	1	1	0	1254
226	1	0	0	0	1	1	1	0	1	0	1	1141	259	1	0	0	1	1	1	0	1	0	0	1	1257
227	1	0	0	0	1	1	1	0	1	1	0	1142	260	1	0	0	1	1	1	0	1	0	1	0	1258
228	1	0	0	0	1	1	1	1	0	0	1	1145	261	1	0	0	1	1	1	0	1	1	0	0	1260
229	1	0	0	0	1	1	1	1	0	1	0	1146	262	1	0	0	1	1	1	1	0	0	0	1	1265
230	1	0	0	0	1	1	1	1	1	0	0	1148	263	1	0	0	1	1	1	1	0	0	1	0	1266

Table 10.1 Continues

Sl. No.	Scientists a b c d e f g h i j k	Binary value	Sl. No.	Scientists a b c d e f g h i j k	Binary value
264	1 0 0 1 1 1 1 0 1 0 0	1268	297	1 0 1 0 1 1 1 0 0 0 1	1393
265	1 0 0 1 1 1 1 1 0 0 0	1272	298	1 0 1 0 1 1 1 0 0 1 0	1394
266	1 0 1 0 0 0 0 1 1 1 1	1295	299	1 0 1 0 1 1 1 0 1 0 0	1396
267	1 0 1 0 0 0 1 0 1 1 1	1303	300	1 0 1 0 1 1 1 1 0 0 0	1400
268	1 0 1 0 0 0 1 1 0 1 1	1307	301	1 0 1 1 0 0 0 0 1 1 1	1415
269	1 0 1 0 0 0 1 1 1 0 1	1309	302	1 0 1 1 0 0 0 1 0 1 1	1419
270	1 0 1 0 0 0 1 1 1 1 0	1310	303	1 0 1 1 0 0 0 1 1 0 1	1421
271	1 0 1 0 0 1 0 0 1 1 1	1319	304	1 0 1 1 0 0 0 1 1 1 0	1422
272	1 0 1 0 0 1 0 1 0 1 1	1323	305	1 0 1 1 0 0 1 0 0 1 1	1427
273	1 0 1 0 0 1 0 1 1 0 1	1325	306	1 0 1 1 0 0 1 0 1 0 1	1429
274	1 0 1 0 0 1 0 1 1 1 0	1326	307	1 0 1 1 0 0 1 0 1 1 0	1430
275	1 0 1 0 0 1 1 0 0 1 1	1331	308	1 0 1 1 0 0 1 1 0 0 1	1433
276	1 0 1 0 0 1 1 0 1 0 1	1333	309	1 0 1 1 0 0 1 1 0 1 0	1434
277	1 0 1 0 0 1 1 0 1 1 0	1334	310	1 0 1 1 0 0 1 1 1 0 0	1436
278	1 0 1 0 0 1 1 1 0 0 1	1337	311	1 0 1 1 0 1 0 0 0 1 1	1443
279	1 0 1 0 0 1 1 1 0 1 0	1338	312	1 0 1 1 0 1 0 0 1 0 1	1445
280	1 0 1 0 0 1 1 1 1 0 0	1340	313	1 0 1 1 0 1 0 0 1 1 0	1446
281	1 0 1 0 1 0 0 0 1 1 1	1351	314	1 0 1 1 0 1 0 1 0 0 1	1449
282	1 0 1 0 1 0 0 1 0 1 1	1355	315	1 0 1 1 0 1 0 1 0 1 0	1450
283	1 0 1 0 1 0 0 1 1 0 1	1357	316	1 0 1 1 0 1 0 1 1 0 0	1452
284	1 0 1 0 1 0 0 1 1 1 0	1358	317	1 0 1 1 0 1 1 0 0 0 1	1457
285	1 0 1 0 1 0 1 0 0 1 1	1363	318	1 0 1 1 0 1 1 0 0 1 0	1458
286	1 0 1 0 1 0 1 0 1 0 1	1365	319	1 0 1 1 0 1 1 0 1 0 0	1460
287	1 0 1 0 1 0 1 0 1 1 0	1366	320	1 0 1 1 0 1 1 1 0 0 0	1464
288	1 0 1 0 1 0 1 1 0 0 1	1369	321	1 0 1 1 1 0 0 0 0 1 1	1475
289	1 0 1 0 1 0 1 1 0 1 0	1370	322	1 0 1 1 1 0 0 0 1 0 1	1477
290	1 0 1 0 1 0 1 1 1 0 0	1372	323	1 0 1 1 1 0 0 0 1 1 0	1478
291	1 0 1 0 1 1 0 0 0 1 1	1379	324	1 0 1 1 1 0 0 1 0 0 1	1481
292	1 0 1 0 1 1 0 0 1 0 1	1381	325	1 0 1 1 1 0 0 1 0 1 0	1482
293	1 0 1 0 1 1 0 0 1 1 0	1382	326	1 0 1 1 1 0 0 1 1 0 0	1484
294	1 0 1 0 1 1 0 1 0 0 1	1385	327	1 0 1 1 1 0 1 0 0 0 1	1489
295	1 0 1 0 1 1 0 1 0 1 0	1386	328	1 0 1 1 1 0 1 0 0 1 0	1490
296	1 0 1 0 1 1 0 1 1 0 0	1388	329	1 0 1 1 1 0 1 0 1 0 0	1492

Table 10.1 Continues

Sl. No.	Scientists a	b	c	d	e	f	g	h	i	j	k	Binary value	Sl. No.	Scientists a	b	c	d	e	f	g	h	i	j	k	Binary value
330	1	0	1	1	1	0	1	1	0	0	0	1496	363	1	1	0	0	1	1	0	0	1	1	0	1638
331	1	0	1	1	1	1	0	0	0	0	1	1505	364	1	1	0	0	1	1	0	1	0	0	1	1641
332	1	0	1	1	1	1	0	0	0	1	0	1506	365	1	1	0	0	1	1	0	1	0	1	0	1642
333	1	0	1	1	1	1	0	0	1	0	0	1508	366	1	1	0	0	1	1	0	1	1	0	0	1644
334	1	0	1	1	1	1	0	1	0	0	0	1512	367	1	1	0	0	1	1	1	0	0	0	1	1649
335	1	0	1	1	1	1	1	0	0	0	0	1520	368	1	1	0	0	1	1	1	0	0	1	0	1650
336	1	1	0	0	0	0	0	1	1	1	1	1551	369	1	1	0	0	1	1	1	0	1	0	0	1652
337	1	1	0	0	0	0	1	0	1	1	1	1559	370	1	1	0	0	1	1	1	1	0	0	0	1656
338	1	1	0	0	0	0	1	1	0	1	1	1563	371	1	1	0	1	0	0	0	0	1	1	1	1671
339	1	1	0	0	0	0	1	1	1	0	1	1565	372	1	1	0	1	0	0	0	1	0	1	1	1675
340	1	1	0	0	0	0	1	1	1	1	0	1566	373	1	1	0	1	0	0	0	1	1	0	1	1677
341	1	1	0	0	0	1	0	0	1	1	1	1575	374	1	1	0	1	0	0	0	1	1	1	0	1678
342	1	1	0	0	0	1	0	1	0	1	1	1579	375	1	1	0	1	0	0	1	0	0	1	1	1683
343	1	1	0	0	0	1	0	1	1	0	1	1581	376	1	1	0	1	0	0	1	0	1	0	1	1685
344	1	1	0	0	0	1	0	1	1	1	0	1582	377	1	1	0	1	0	0	1	0	1	1	0	1686
345	1	1	0	0	0	1	1	0	0	1	1	1587	378	1	1	0	1	0	0	1	1	0	0	1	1689
346	1	1	0	0	0	1	1	0	1	0	1	1589	379	1	1	0	1	0	0	1	1	0	1	0	1690
347	1	1	0	0	0	1	1	0	1	1	0	1590	380	1	1	0	1	0	0	1	1	1	0	0	1692
348	1	1	0	0	0	1	1	1	0	0	1	1593	381	1	1	0	1	0	1	0	0	0	1	1	1699
349	1	1	0	0	0	1	1	1	0	1	0	1594	382	1	1	0	1	0	1	0	0	1	0	1	1701
350	1	1	0	0	0	1	1	1	1	0	0	1596	383	1	1	0	1	0	1	0	0	1	1	0	1702
351	1	1	0	0	1	0	0	0	1	1	1	1607	384	1	1	0	1	0	1	0	1	0	0	1	1705
352	1	1	0	0	1	0	0	1	0	1	1	1611	385	1	1	0	1	0	1	0	1	0	1	0	1706
353	1	1	0	0	1	0	0	1	1	0	1	1613	386	1	1	0	1	0	1	0	1	1	0	0	1708
354	1	1	0	0	1	0	0	1	1	1	0	1614	387	1	1	0	1	0	1	1	0	0	0	1	1713
355	1	1	0	0	1	0	1	0	0	1	1	1619	388	1	1	0	1	0	1	1	0	0	1	0	1714
356	1	1	0	0	1	0	1	0	1	0	1	1621	389	1	1	0	1	0	1	1	0	1	0	0	1716
357	1	1	0	0	1	0	1	0	1	1	0	1622	390	1	1	0	1	0	1	1	1	0	0	0	1720
358	1	1	0	0	1	0	1	1	0	0	1	1625	391	1	1	0	1	1	0	0	0	0	1	1	1731
359	1	1	0	0	1	0	1	1	0	1	0	1626	392	1	1	0	1	1	0	0	0	1	0	1	1733
360	1	1	0	0	1	0	1	1	1	0	0	1628	393	1	1	0	1	1	0	0	0	1	1	0	1734
361	1	1	0	0	1	1	0	0	0	1	1	1635	394	1	1	0	1	1	0	0	1	0	0	1	1737
362	1	1	0	0	1	1	0	0	1	0	1	1637	395	1	1	0	1	1	0	0	1	0	1	0	1738

Table 10.1 Continues

Sl. No.	Scientists a b c d e f g h i j k	Binary value	Sl. No.	Scientists a b c d e f g h i j k	Binary value
396	1 1 0 1 1 0 0 1 1 0 0	1740	429	1 1 1 0 1 0 0 1 0 0 1	1865
397	1 1 0 1 1 0 1 0 0 0 1	1745	430	1 1 1 0 1 0 0 1 0 1 0	1866
398	1 1 0 1 1 0 1 0 0 1 0	1746	431	1 1 1 0 1 0 0 1 1 0 0	1868
399	1 1 0 1 1 0 1 0 1 0 0	1748	432	1 1 1 0 1 0 1 0 0 0 1	1873
400	1 1 0 1 1 0 1 1 0 0 0	1752	433	1 1 1 0 1 0 1 0 0 1 0	1874
401	1 1 0 1 1 1 0 0 0 0 1	1761	434	1 1 1 0 1 0 1 0 1 0 0	1876
402	1 1 0 1 1 1 0 0 0 1 0	1762	435	1 1 1 0 1 0 1 1 0 0 0	1880
403	1 1 0 1 1 1 0 0 1 0 0	1764	436	1 1 1 0 1 1 0 0 0 0 1	1889
404	1 1 0 1 1 1 0 1 0 0 0	1768	437	1 1 1 0 1 1 0 0 0 1 0	1890
405	1 1 0 1 1 1 1 0 0 0 0	1776	438	1 1 1 0 1 1 0 0 1 0 0	1892
406	1 1 1 0 0 0 0 0 1 1 1	1799	439	1 1 1 0 1 1 0 1 0 0 0	1896
407	1 1 1 0 0 0 0 1 0 1 1	1803	440	1 1 1 0 1 1 1 0 0 0 0	1904
408	1 1 1 0 0 0 0 1 1 0 1	1805	441	1 1 1 1 0 0 0 0 0 1 1	1923
409	1 1 1 0 0 0 0 1 1 1 0	1806	442	1 1 1 1 0 0 0 0 1 0 1	1925
410	1 1 1 0 0 0 1 0 0 1 1	1811	443	1 1 1 1 0 0 0 0 1 1 0	1926
411	1 1 1 0 0 0 1 0 1 0 1	1813	444	1 1 1 1 0 0 0 1 0 0 1	1929
412	1 1 1 0 0 0 1 0 1 1 0	1814	445	1 1 1 1 0 0 0 1 0 1 0	1930
413	1 1 1 0 0 0 1 1 0 0 1	1817	446	1 1 1 1 0 0 0 1 1 0 0	1932
414	1 1 1 0 0 0 1 1 0 1 0	1818	447	1 1 1 1 0 0 1 0 0 0 1	1937
415	1 1 1 0 0 0 1 1 1 0 0	1820	448	1 1 1 1 0 0 1 0 0 1 0	1938
416	1 1 1 0 0 1 0 0 0 1 1	1827	449	1 1 1 1 0 0 1 0 1 0 0	1940
417	1 1 1 0 0 1 0 0 1 0 1	1829	450	1 1 1 1 0 0 1 1 0 0 0	1944
418	1 1 1 0 0 1 0 0 1 1 0	1830	451	1 1 1 1 0 1 0 0 0 0 1	1953
419	1 1 1 0 0 1 0 1 0 0 1	1833	452	1 1 1 1 0 1 0 0 0 1 0	1954
420	1 1 1 0 0 1 0 1 0 1 0	1834	453	1 1 1 1 0 1 0 0 1 0 0	1956
421	1 1 1 0 0 1 0 1 1 0 0	1836	454	1 1 1 1 0 1 0 1 0 0 0	1960
422	1 1 1 0 0 1 1 0 0 0 1	1841	455	1 1 1 1 0 1 1 0 0 0 0	1968
423	1 1 1 0 0 1 1 0 0 1 0	1842	456	1 1 1 1 1 0 0 0 0 0 1	1985
424	1 1 1 0 0 1 1 0 1 0 0	1844	457	1 1 1 1 1 0 0 0 0 1 0	1986
425	1 1 1 0 0 1 1 1 0 0 0	1848	458	1 1 1 1 1 0 0 0 1 0 0	1988
426	1 1 1 0 1 0 0 0 0 1 1	1859	459	1 1 1 1 1 0 0 1 0 0 0	1992
427	1 1 1 0 1 0 0 0 1 0 1	1861	460	1 1 1 1 1 0 1 0 0 0 0	2000
428	1 1 1 0 1 0 0 0 1 1 0	1862	461	1 1 1 1 1 1 0 0 0 0 0	2016

APPENDIX 2

The Extended Euclidean Algorithm

Suppose a and b are positive integers and d be their greatest common divisor. We know that the g.c.d can be written as a linear combination of the numbers. S, there exists integers x and y, such that,

$$ax + by = d \tag{10.1}$$

It may be noted that, except in some trivial cases, x and y will be of opposite signs. If x and y satisfies equation (10.1), so is $(x+qb)$ and $(y-qa)$, for any integer q. So, one can always find integers x any y, with $x > 0$ and $y < 0$, which satisfies the equation (10.1).

The *Extended Euclidean Algorithm* will calculate d, and also two integers x and y, such that $ax+by = d$ at the same time. This explains why the resulting procedure is known as the Extended Euclidean Algorithm. The version of the algorithm we present here is the creation of D. E. Knuth, author of the famous book *The Art of Computer Programming*. The Algorithm can be found in volume 2 of the series; (see Knuth [40]. section 4.5.2, algorithm X.)

Algorithm 10.1 (Extended Euclidean Algorithm)

Input : Two positive integers a and b.

Output: Three integers d, x, and y such that equation (10.1) holds good.

Step 1. *Initialize* $x = 0, y = 1$

$c = a, d = b$

Step 2. *Repeat*

$r = c \pmod{d}$

$q = (c - r)/d$

if $(r = 0)$ *GO TO Step 3.*

$t = x$

$x = y - x * q$

$y = t$

$c = d$

$d = r$

Step 3. $y = (d - a * x)/b$

Step 4. *The numbers x and y satisfies*

$ax + by = d = G.C.D(a, b)$

If G.C.D$(a, b) = 1$, then $ax + by = d$ becomes $ax \equiv 1 \pmod{b}$ and $by \equiv 1 \pmod{a}$. So, $a^{-1} \equiv x \pmod{b}$, as well as $b^{-1} \equiv y \pmod{a}$. We can use the above algorithm to find out the inverse, whenever it exists.

Example 10.1

Let us find the inverse of $655 \pmod{1234}, 655^{-1} \pmod{1234}$

The following table shows the values of the variables r, q, and x at 3^{rd} line in each iteration of Step 2.
Step 3 evaluates $y = 341$, which is the inverse of $655 \pmod{1234}$.

Table 10.2: Illustration of Extended Euclidean Algorithm

Iteration Number	Remainders (r)	Quotients (q)	(x)
1	579	1	0
2	76	1	1
3	47	7	-1
4	29	1	8
5	18	1	-9
6	11	1	17
7	7	1	-26
8	4	1	43
9	3	1	-69
10	1	1	112
11	0	3	-181

APPENDIX 3

List of Research Papers

Published Papers :

1. Uniform Secret Sharing Schemes for (2, n) Threshold
   Using Visual Cryptography:
   International Journal of Information Processing,
   Volume 2, Number 4, 2008 pp 82- 87.

2. International Conference held at I.I.T., Kanpur. The paper is available in the web-site of the conference at pages: 33 to 37. The URL is

   http://www.security.iitk.ac.in/hack.in/2009/repository/proceedings_hack.in.pdf

Accepted Papers:

3. An Efficient Secret Sharing Scheme for n out of n scheme
   using POB-number system:
   Journal of Discrete Mathematical Sciences and Cryptography

4. An Effective Secret Sharing Scheme for n out of n scheme
   using modified Visual cryptography:
   Journal of Computer Science

Communicated papers:

5. An Efficient Secret Sharing Scheme for $(n-1, n)$ threshold
   using Visual cryptography:
   International Journal of Information Processing.

APPENDIX 4

SYNOPSIS of the Ph. D. thesis

Submitted by
A. Sreekumar, Research Scholar (Part-time),
Department of Computer Applications,
Cochin University of Science and Technology,

Under the guidance of
Professor, Dr. S. Babusundar

Topic: **CRYPTOGRAPHY**

Title: **Secret Sharing Schemes using Visual Cryptography**

1. Introduction

Handling secret has been an issue of prominence from the time human beings started to live together. Important things and messages have been always there to be preserved and protected from possible misuse or loss. Some time secret is thought to be secure in a single hand and at other times it is thought to be secure when shared in many hands. Some of the formulae of vital combinations of medicinal plants or roots or leaves, in

Ayurveda were known to a single person in a family. When he becomes old enough, he would rather share the secret formula to a chosen person from the family, or from among his disciples. There were times when the person with the secret dies before he could share the secret. Probably, similar incidents might have made the genius of those era to think of sharing the secrets with more than one person so that in the event of death of the present custodian, there will be at least one other person who knows the secret.

Secret sharing in other forms were prevailing in the past, for other reasons also. Secrets were divided into number of pieces and given to the same number of people. To ensure unity among the participating people, the head of the family would share the information with respect to wealth among his children and insist that after his death, they all should join together to inherit the wealth.

To test the valor of the youth of a nation, a king, would hide treasure in some place in his kingdom and information about it would be placed in pieces at different places of varying grades of difficulty to reach. Only the brave and the intelligent would reach the treasure.

Military and defense secrets have been the subject matter for secret sharing in the past as well as in the modern days. Secret sharing is a very hot area of research in Computer Science in

the recent past. Digital media has replaced almost all forms of communication and information preservation and processing. Security in digital media has been a matter of serious concern. This has resulted in the development of encryption and cryptography. Uniform secret sharing schemes form a part of this large study.

1.1 Definition: A Secret sharing scheme is a method of dividing a secret information into two or more pieces, with or without modifications, and retrieving the information by combining all or predefined sub collection of pieces.

The pieces of information are called **shares** and the process responsible for the division is called **dealer**. A predefined sub collection of shares which contains the whole secret in some form is called an **allowed coalition**. The process responsible for the recovery of the secret information from an allowed coalition is called a **combiner**.

A share contains, logically, a part of the information, but will be of no use. Thus no single share is of any threat to the confidentiality of the secret information. It is also envisaged that after the dealer process is over, the original information can be destroyed forever. This would mean that even the person responsible for the dealer process will not be a threat, thereafter. The secret information is recovered from any allowed coalition using the recovery process called combiner. The combiner would be able to recover the secret information, only if, all shares in

the allowed coalition is present and not with any fewer number of shares. Thus, in an allowed coalition, each member share is equally important such that without anyone of them, the secret information cannot be accessed.

Allowed coalition is also referred in the literature by other names too, such as, **authentic collection**, **qualified collection** or **authorized set**. We, in our work, preferred to call the sub collection of shares as allowed coalition.

Secret Sharing is an important tool in Security and Cryptography. In many cases there is a single master key that provides the access to important secret information. Therefore, it would be desirable to keep the master key in a safe place to avoid accidental and malicious exposure. This scheme is unreliable: if master key is lost or destroyed, then all information accessed by the master key is no longer available. A possible solution would be that of storing copies of the key in different safe places or giving copies to trusted people. In such a case the system becomes more vulnerable to security breaches or betrayal [53], [30]. A better solution would be, breaking the master key into pieces in such a way that only the concurrence of certain predefined trusted people can recover it. This has proven to be an important tool in management of cryptographic keys and multi-party secure protocols (see for example [33]).

As a solution to this problem, Blakley [9] and Shamir [53] introduced $(k,\ n)$ threshold schemes. A $(k,\ n)$ threshold scheme

allows a secret to be shared among n participants, in such a way that, any k of them can recover the secret, but $k-1$, or fewer, have absolutely no information on the secret.

Ito, Saito, and Nishizeki [36] described a more general method of secret sharing. An access structure is a specification of all subsets of participants who can recover the secret and it is said to be monotone if any set which contains a subset that can recover the secret, can itself recover the secret. Ito, Saito, and Nishizeki gave a methodology to realize secret sharing schemes for arbitrary monotone access structures. Subsequently, Benaloh and Leichter [5] gave a simpler and more efficient way to realize such schemes.

An important issue in the implementation of secret sharing scheme is the size of the shares distributed to the participants, since the security of a system degrades as the amount of the information that must be kept secret increases. So the size of the shares given to the participants is a key point in the design of secret sharing schemes. Therefore, one of the main parameters in secret sharing is, the **average information rate** ρ, of the scheme, which is defined as the ratio between the average length (in bits) of the shares given to the participants and the length of the secret. Unfortunately, in all secret sharing schemes the size of the shares cannot be less than the size of the secret, and so the information rate cannot be less than one. Moreover, there are access structures, for which, any corresponding secret

sharing scheme must give to some participant a share of size strictly bigger than the secret size. Secret sharing schemes with information rate equal to one are called **ideal**. A secret sharing scheme is called efficient if the total length of the n shares is polynomial in n.

2. Model of secret sharing

A common model of secret sharing has two phases. In the initialization phase, a trusted entity - the dealer, divides the secret information into shares and distributes the shares by secure means. In the reconstruction phase one of the allowed coalition submit their shares to a combiner, who reconstructs the secret. It is assumed that the combiner is an algorithm which only performs the task of reconstructing the secret. Various Secret Sharing Schemes have been proposed since 1979. The following are some of the known schemes:

1. Blakley's scheme using projective spaces over finite fields GF(q)
2. Simmons' scheme in terms of affine spaces
3. Shamir's scheme based on polynomial interpolation over finite fields.

In most of the schemes, when a great number of participants are involved, the scheme will become impractical. In the traditional

Secret Sharing Schemes, a shared secret information cannot be revealed without any cryptographic computations.

2.1 Visual Cryptography There are various connections between combinatorial structures and secret sharing. For example, a (2, 3) threshold scheme can be implemented based on a small Latin square. In 1994, Naor and Shamir invented a new type of secret sharing scheme, called Visual Cryptography scheme [48]. In secret sharing schemes using Visual Cryptography, a shared secret information (printed text, handwritten notes, pictures, etc.) can be revealed without any cryptographic computations. For example, in a (k, n) visual cryptography scheme, a dealer encodes a secret into n shares and gives each participant a share, where each share is a transparency. The secret is visible if any k (or more) of participants stack their transparencies together, but none can see the shared secret if fewer than k transparencies are stacked together.

3. Problem specification

Secret sharing is one of the cryptographic techniques providing security measures to protect information. Due to difficulty of finding a general solution, those problems have been studied in several particular cases, and several sharing schemes have been proposed. So this particular work focuses on a generalized scheme, for at least some values of k, which works with any number of participants.

4. Objective and scope of this Research

Most of the business organizations need to protect data from disclosure. As the world is more connected by computers, the hackers, power abusers have also increased, and most organizations are afraid to store data in a computer. So there is a need of a method to distribute the data at several places and destroy the original one. When a need of original data arises, it could be reconstructed from the distributed shares. The primitive objective of this research is to provide a solution to this problem.

5. Contribution of the Thesis

The research work provides a better mechanism for secure storage of information. The thesis work proceeds into three phases.

1. The first phase deals with studies and findings in the area of secret sharing.
2. The second phase of the work relates to investigating new structures suitable for specific applications.
3. The third phase deals with the mathematical proofs of the new findings.

6. Design of the scheme

In this research work, we considered a special type of codes, called Uniform Codes to propose sharing schemes. A string of 0s

and 1s is called a uniform code, if the number of 1's is either equal to or one more than the number of 0's. For example, 011010 and 1101001 are uniform codes where as 001 and 110110 are not. It can be seen that, if the length of a binary string is w, then the number of codes having length w, and having t 1's is $\binom{\mathrm{w}}{\mathrm{t}}$. For a given w, this number is maximum when $t = \left\lfloor \frac{n}{2} \right\rfloor$, the integer part of $\frac{n}{2}$. So the maximum number of codes with a given length occurs when they are uniform. Four efficient threshold schemes are proposed based on Modified Visual Cryptography introduced in 2002. All the schemes are based on the uniform codes. The first scheme proposed is an efficient (2, n) threshold scheme. This scheme provides an efficient way to hide a secret information in different shares, in which the size of the shares is just in $O(log_2\ n)$ times the original secret size, where n is the number of participants. The second scheme is a (3, n) threshold scheme in which the size of the shares is just in $O(n)$ times the original secret size, where n is the number of participants. The third scheme is $(n-1,\ n)$ threshold scheme in which the size of the share is in $O(n/2)$. We have generalized the concept of Uniform code by relaxing the constraints, and introduced a new number system, called *Permutation Ordered Number System* (or POB-Number system). The system has two parameters. We have developed some algorithms for efficiently representing the usual numbers in the new system, and vice-versa. Finally we found that a certain class of binary strings can be decomposed in the

class of balanced strings, and Uniform Codes. By using the POB-Number system, we can represent Uniform codes and balanced strings effectively. We exploit this property, and developed an efficient sharing algorithm in which the size of the share is less than the size of the secret. We have come across the following finding: Let w be an even parity string and $n_1(w)$ denotes the number of 1's in a binary string w of length t. Then w can be written as $w = S_1 \oplus S_2 \oplus \ldots \oplus S_n,$, where, S_i is a Uniform Code, for each $i = 1,\ 2, \ldots,\ n$. Here $\oplus$ is the usual bitwise XOR operation. We have developed all the algorithms and illustrated them with appropriate examples. This scheme is very efficient, as the size of the share is less than the size of the original secret, in which we have a gain of 1/8.

7. Content of the thesis

The thesis is presented in 10 chapters. We have taken care to provide a good account of the literature survey and the theoretical background of the topic of study. All the details of the development of the newly proposed algorithms and the proofs of the claim are also included. Some of the algorithms have been presented, either in full or in parts, in conferences and journals. An account of these publications are also included.

The first chapter deals with the introduction. It contains the sketch of the development and progress of the topic of study.

The Second chapter deals with history and literature survey.

The Third chapter deals with the visual cryptography and its examples.

The Fourth chapter deals with modified cryptography.

The next four chapters deal with the solutions proposed by us, which is our contribution to this area of study. The findings are presented in conferences and others are either published or accepted for publication in journals. One of our research paper is published in the International Journal of Information Processing, Volume 2, Number 4, 2008 pp 82-87.

Another two papers are accepted for publication, and will be published within one month. A fifth paper is communicated for publication. The result is awaited. The details are included in the thesis

As a good by-product of this research work, we have developed a new number system. It is named as *Permutation Oriented Binary Number System* (**POB-number system**). In an International Conference at I.I.T., Kanpur, we have presented this part of the research work. The paper was one among the eleven selected papers out of a total of 40 research papers, submitted, in the areas of Cryptography and Network Security. We are happy to say that, our paper was ranked fourth among the 10 papers presented there. The paper is available in the web-site of the conference at pages: 33 to 37. The url is

http://www.security.iitk.ac.in/hack.in/2009/repository/proceedings_hack.in.pdf

The Ninth chapter deals with the most important result we have achieved. We have developed an algorithm, in which the secret could be shared among n participants with a single allowed coalition such that the size of the share is less the size of the secret message. The final chapter deals with the probable direction of future research work in this area.