

Geometric Shared Secret and/or Shared Control Schemes*

*Gustavus J. Simmons
Sandia National Laboratories
Albuquerque, New Mexico 87185, USA*

Introduction

A shared secret scheme is normally specified in terms of a desired security, P_d , and a concurrence scheme, Γ . The concurrence scheme (aka access structure) identifies subsets of participants (also called trustees or shareholders) each of which should be able to cooperatively recover the secret and/or initiate the controlled action. The security requirement is expressed as the maximum acceptable probability, P_d , that the secret can be exposed or the controlled action initiated by a collection of persons that doesn't include at least one of the authorized subsets identified in the concurrence scheme. A concurrence scheme is said to be monotone if every set of participants that includes one or more sets from Γ is also able to recover the secret. The closure of Γ , denoted by $\hat{\Gamma}$, is the collection of all supersets (not necessarily proper) of the sets in Γ , i.e., the collection of all sets of participants that can recover the secret and/or initiate the controlled action. A shared secret scheme implementing a concurrence scheme Γ is said to be perfect if the probability of recovering the secret is the same for every set, C , of participants: $C \in \hat{\Gamma}$. Since, in particular, C could consist of only nonparticipants, i.e., of persons with no insider information about the secret, the probability, P , of an unauthorized recovery of the secret in a perfect scheme is just the probability of being able to "guess" the secret using only public information about Γ and the shared secret scheme implementing Γ : $P \leq P_d$. A shared secret scheme is said to be unconditionally secure if P is independent of the computing power or effort that the opponent(s) may be willing to expend in an effort to improperly recover the secret.

* This work performed at Sandia National Laboratories supported by the U. S. Department of Energy under contract no. DE-AC04-76DP00789.

Our convention will be that the secret is a point, p , in a publicly known space V_d , and that every point in this space is a priori equally likely to be the secret. This says that

$$|V_d| \geq \frac{1}{P_d}$$

i.e., that the minimum cardinality of V_d is determined by the security requirements. V_d is considered to be embedded in another space S , where—except in the degenerate case in which each of the participants can unilaterally initiate the controlled action— S will be of higher dimension than V_d :

$$\dim(S) = n > \dim(V_d) = m \quad .$$

At each point in V_d , there will be the same number of $(n-m)$ -dimensional subspaces of S each of which has only that point in common with V_d . A point p in V_d and one of the $(n-m)$ -dimensional subspaces, V_i , lying on p are chosen randomly and with a uniform probability distribution. The subspace V_i is called the indicator since given it and knowing V_d , p can be easily identified, i.e., V_i indicates or points to the point p in V_d . Conversely, given V_d and any subspace disjoint from V_d , because of the way in which p was chosen, p can only be "guessed" at with a probability of success (on the first try) of

$$P = \frac{1}{|V_d|} \leq P_d \quad .$$

A perfect (monotone) geometric shared secret scheme implementing the concurrence scheme Γ is an assignment of subspaces (algebraic varieties in general) of V_i to the participants in such a way that the collection of subspaces held by any set of participants \mathbf{C} , $\mathbf{C} \in \Gamma$, span V_i and hence indicate p , while the space spanned by the collection of subspaces held by a set \mathbf{D} , for every $\mathbf{D} \notin \hat{\Gamma}$, is disjoint from V_d and hence yields no information whatsoever about p . While it may not be obvious, it is at least plausible—and as it happens, true—that the minimum dimension of V_i is determined by the concurrence scheme Γ . Thus, since the security requirement only determines the minimum cardinality of V_d and the concurrence scheme the minimum dimension of V_i , it should be no

surprise that the specifications for a shared control scheme do not uniquely define a geometric shared secret scheme.

While it isn't really necessary to exhibit an example to understand the implications of the preceding remark, an example does make it easier to see why the designer of a shared control scheme might choose one realization in preference to others. Consider a simple 2-out-of-4 threshold scheme (also called a $(2,4)$ threshold scheme) for which the specified security is $P_d \leq 10^{-6}$, i.e., for which the chance of an outsider or any participant alone guessing the secret on their first try will be no greater than one in a million. This says that the subspace in which the secret is concealed must contain at least a million points. Since we wish to work with finite geometries coordinatized by finite fields, a natural choice in this case would be to work with an extension field over $GF(2)$ since $2^{20} = 1,048,576$. The dimension of the indicator subspace must be at least one since the lowest dimensional realization of an indicator for a 2-out-of-4 threshold scheme consists of four distinct points on a line (the minimum dimension of V_i is determined by Γ). Figure 1 shows two possible realizations in this case.

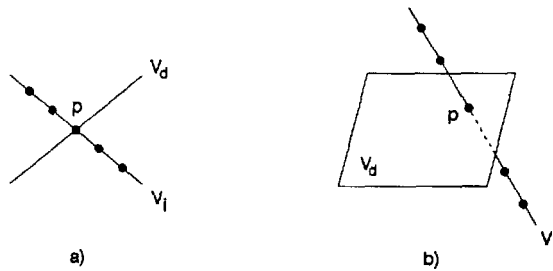


Figure 1.

In (a), since $|V_d| = 2^{20}$, $q = 2^{20}$. Consequently ≈ 40 bits¹ of information will be required to identify a point (the private pieces of information) in the plane, S , containing V_d and V_i . On the other hand, in (b), $q = 2^{10}$ since V_d is 2-dimensional. S is 3-dimensional in this case, so that the private pieces of information need only be ≈ 30 bits in size. V_d could also be chosen to be 5-dimensional (over $GF(2^4)$) in

1. If the constructions are in $AG(n, q)$, then the information content of the private pieces of information will be equal to $n \log_2(q)$. If $S = PG(n, q)$ the number of points in the space is $(q^{n+1}-1)/(q-1)$ instead of q^n , so that the number of bits required to specify a point will be larger than $n \log_2(q)$.

which case S would be 6-dimensional and the private pieces of information would consist of ≈ 24 bits. This is the most economical construction possible for this example in an affine geometry since if V_d were made to be 10-dimensional (over $GF(2^2)$) there would only be four points on a line. On the indicator line V_i , one of these would have to be the point p . Hence, it would be impossible to assign four distinct points as the private pieces of information, each of which would also have to be distinct from p , as required in the specification of the desired shared control. The scheme could just be fitted into $PG(11,2^2)$ since in this case there are five points on each line. This would be slightly more economical of information—saving epsilon more than one bit. However, the first point that we wanted to make with this example should be clear; namely, that even after the indicator V_i has been chosen, the designer may still have a choice of V_d to make depending on considerations other than just the specification of P_d and Γ .

A more interesting freedom exists in the choice of V_i in the first place. Even for this very simple concurrence scheme (Γ a 2-out-of-4 threshold scheme) there are infinitely many choices for V_i . All that is required is that there be at least four distinct and proper subspaces of V_i any two of which span V_i and no one of which lies on the specified point p in V_i . The smallest such example consisted of four distinct points on a line containing at least five points. Figure 2 shows three low-dimensional possible choices for V_i .

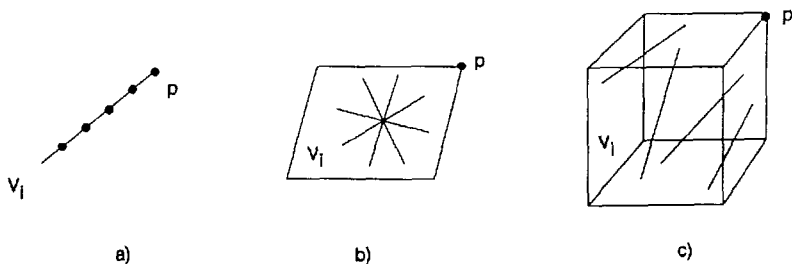


Figure 2.

(a) we have already discussed at length. In (b) the private pieces of information are four lines in the plane V_i , no one of which lies on the point p (they need not be concurrent as shown). In (c) the private pieces of information are four pairwise skew lines in the 3-space V_i , no

one of which lies on the point p . Obviously there are infinitely many choices for the space V_i and associated spanning set of subspaces—what isn't obvious is why the designer would ever chose to use anything other than the minimal dimensional realization of Γ . To illustrate this, one must consider more complex concurrences than simple threshold schemes. The treatment of these more general—and complicated—concurrency schemes is the primary objective of this paper, so we will defer the discussion of these considerations until later. The second point that we wanted to make with this example was to illustrate the freedom of choice for V_i which is also available to the designer of a shared control scheme.

We should remark at this point, that in this paper we will only be concerned with unconditionally secure perfect monotone geometric shared secret schemes.

The Geometry of Concurrency Schemes

When there are only two participants in a shared control scheme, there are only two types of control possible: either it is possible for either one of them to initiate the controlled action unilaterally, or else it requires the concurrence of both of them to do so. The first situation corresponds to two persons knowing the combination to a conventional safe so that either of them can open it, while the second corresponds to the U.S. military's common usage of safes with two separate combination locks for securing critical command and control information. In this case, two responsible officers each know the combination to one and only one of the locks, both of which must be unlocked in order for the safe to be opened.

Our conventions will be to represent participants with capital letters A, B, \dots , etc., and to use standard logical notation, (\cdot) to denote conjunction and $+$ to denote or, to express concurrences. For the case of two participants, $n = 2$, we therefore have the pair of concurrence schemes:

$$\Gamma = A + B \quad \text{and} \quad \Gamma = AB \quad .$$

These may be represented graphically

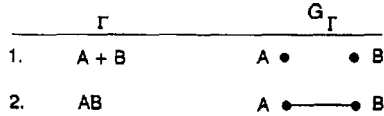


Figure 3.

with the edge AB in the right-hand figure indicating that A and B (denoted by $A \bullet B$ or AB) must concur in order for the controlled event to be initiated.

For $n = 3$, the situation is somewhat more interesting since in this case there are five possible equivalence classes of concurrence schemes (up to a permutation of the labels for the participants):

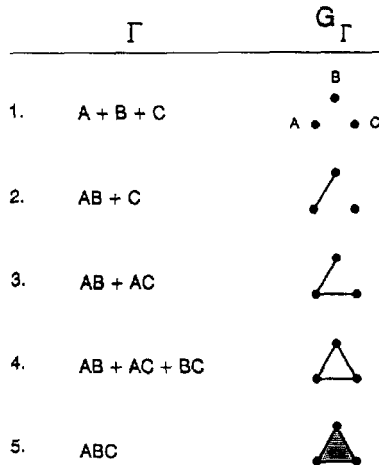


Figure 4.

The unlabeled graphs in the right-hand column, G_Γ , correspond to equivalence classes of concurrence schemes. The concurrence schemes shown in the column, Γ , are the specific member of the class obtained with the indicated labeling for the participants.

Observation: There is a natural one-to-one correspondence between the set of isomorphism classes of monotone concurrence schemes involving n participants and the set of hypergraphs on n vertices; subject to the condition that no hyperedge properly contains any other edge of the graph. To see this, label the vertices with the participants and include as an edge in G any subset, C , of participants that appears in the concurrence scheme Γ , i.e., $C \in \Gamma$. Conversely, given a hypergraph

G , the associated concurrence scheme Γ is simply an enumeration of the edges of G . The utility of this correspondence is that it provides a convenient representation for the equivalence classes of concurrence schemes, independent of a particular labeling.



represents a 2-out-of-4 threshold scheme which already has a concise description. However



represents a concurrence scheme in which any pair out of a set of three participants, in concurrence with a specified fourth participant, can initiate the controlled action. The fourth participant has a kind of veto power in the sense that his input is required in order for the controlled event to be initiated (all three of the other participants together cannot initiate the controlled event). However in spite of this absolute veto power, he cannot unilaterally initiate the controlled action not even in concurrence with one of the other participants. An application for this sort of shared control might very reasonably arise in connection with a treaty controlled action, say between the U.S. and three of its allies where the U.S. wants to retain the right to veto the action, but the allies wish to be guaranteed that at least two of them must agree before the event can be initiated. The reader can now appreciate the utility of the graphical representation which concisely expresses everything that has been said about this concurrence scheme.

Figure 5 shows the twenty concurrence schemes possible for four participants. The column headed Γ shows a canonical representative of each class corresponding to the labeling of vertices shown in 1. The schemes with concise descriptions are 1, 11, 19 and 20 corresponding to (1,4), (2,4), (3,4) and (4,4) threshold schemes, respectively. Many of the others have no concise description as we have already seen for concurrence scheme number 18.

Γ	G_Γ
1. $A + B + C + D$	
2. $AB + C + D$	
3. $AB + CD$	
4. $AB + BC + D$	
5. $AB + BC + CD$	
6. $AB + BC + AC + D$	
7. $AB + AC + AD$	
8. $AB + BC + CD + AD$	
9. $AB + BC + AC + CD$	
10. $AB + AC + AD + BC + CD$	
11. $AB+AC+AD+BC+BD+CD$	
12. $ABC + D$	
13. $ABC + AD$	

Figure 5.

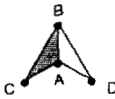




	Γ	G_{Γ}
14.	$ABC + AD + BD$	
15.	$ABC + AD + BD + CD$	
16.	$ABC + ABD$	
17.	$ABC + ABD + CD$	
18.	$ABC + ABD + ACD$	
19.	$ABC + ABD + ACD + BCD$	
20.	$ABCD$	

Figure 5. (cont'd)

Constructing Geometric Shared Secret Schemes

If the desired concurrence scheme is simple enough, a geometric shared secret scheme realizing it may be obvious. This is certainly the case for the two schemes involving only two participants:


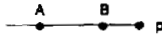
	Γ	S_{Γ}
1.	$A+B$	
2.	AB	

Figure 6.

Geometric shared secret schemes realizing the five possible concurrence schemes with three participants are almost equally obvious:

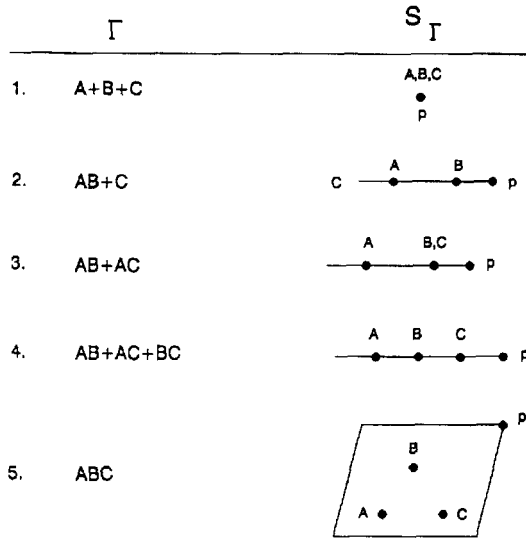


Figure 7.

In general, this will not be the case, though, and formal means for constructing geometric schemes are needed. For example, it is far from obvious how to construct shared secret schemes realizing several of the concurrence schemes shown in Figure 5. To verify this claim, the reader may wish to try to construct schemes realizing concurrences 13, 14 and 17 before reading further.

We will use concurrence scheme #5 from Figure 5 as an example. This scheme was first discussed by Benaloh and Leichter [1] who used it to prove that not every concurrence scheme (which they call an access structure) can be realized by an ideal secret sharing scheme.² While it isn't too difficult to devise a geometric shared secret scheme realizing Γ , a construction certainly isn't obvious either. Assume that V_i is 3-dimensional, then one possible scheme is:

2. A shared secret scheme is said to be ideal if all of the private pieces of information come from the same domain as the secret; i.e., if they are all points in the same space.

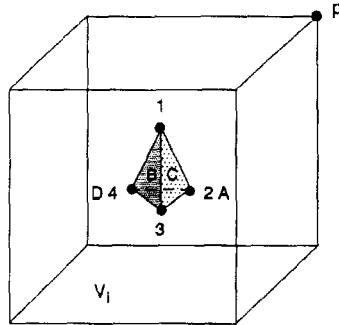
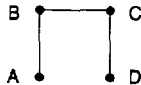


Figure 8.

The four points 1, 2, 3 and 4 are chosen to be in general position and hence they define four planes in V_1 , none of which may lie on the point p . A and D are given points 2 and 4, respectively, as their private pieces of information. B and C are given the planes lying on the triples of points 1, 3 and 4 and 1, 2 and 3, respectively. Clearly the subspaces held by A and B or by B and C, or by C and D span V_1 . Equally clearly V_1 is not spanned by the subspaces held by any other pair of the participants. A's point is in the plane held by C, which by construction does not lie on p . Similarly, D's point is in the plane held by B, etc. Points 2 and 4 (held by A and D) define a line that lies in two planes neither of which lies on p , and hence the line does not lie on p either. Therefore, the configuration shown in Figure 6 is a perfect monotone geometric shared secret scheme realizing the Benaloh-Leichter concurrence.

G_Γ can be redrawn to emphasize its symmetry



It is easy to see that G_Γ and S_Γ have the same symmetry, i.e., they have the same automorphism group. This is also true for the other small examples (of G_Γ , S_Γ pairs) we have seen thus far. It seems plausible, and one might be tempted to conjecture, that for any concurrence scheme Γ , G_Γ and S_Γ will have the same automorphism group. If this were true it would be a powerful tool for the construction of S_Γ . Unfortunately,

the statement is not true as the following alternate geometric realization of the Benaloh-Leichter concurrence shows:

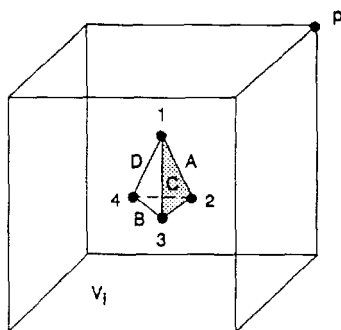


Figure 9.

The assignment of the private pieces of information are: A is given the line defined by points 1 and 2— $\langle 1,2 \rangle$, B the line $\langle 3,4 \rangle$, C the plane $\langle 1,2,3 \rangle$ and D the line $\langle 1,4 \rangle$. It is easy to see that this is also a perfect monotone geometric shared secret scheme realizing the Benaloh-Leichter concurrence, but completely lacking the symmetry of G_Γ .

The primary objective in this section is the statement and illustration of several observations about shared secret schemes based on properties of the associated concurrence schemes. We will dignify these—because of their usefulness—by calling them theorems, although their validity is generally self-evident.

Theorem 1. If the hypergraph G_Γ representing the concurrence scheme Γ is disjoint, then a geometric shared secret scheme, S_Γ , can be constructed as the union of independent geometric shared secret schemes realizing each of the components—all indicating the same point p in V_d however.

Theorem 1 can be applied to concurrence scheme 3 in Figure 5:

$$\Gamma = AB + CD \quad .$$

Since there are two components to G_Γ , there will be two indicators in a shared secret scheme constructed using Theorem 1; both indicating the point p in V_d , of course.

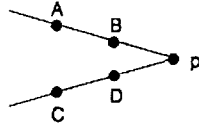


Figure 10.

It is interesting to compare this simple realization to one involving only a single indicator subspace; i.e., to a construction made without the aid of Theorem 1.

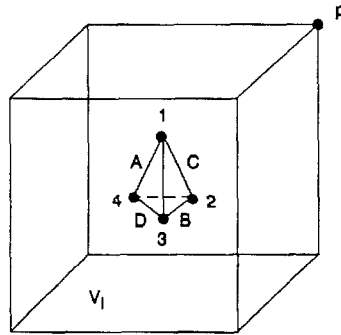


Figure 11.

We know of no simpler realization of Γ using only a single indicator. The simplification resulting from applying Theorem 1, while illustrated by this small example, can be dramatic for more complex concurrence schemes.

It should be remarked at this point that Ito, Saito and Nishizeki [6] first proved that every concurrence scheme can be realized by a perfect (nongeometric) shared secret scheme using a construction similar to those made using Theorem 1. Given a concurrence Γ in disjunctive normal form (a sum of products of the literals), they construct an independent shared secret scheme—revealing the same secret, of course—for each term (product) in Γ . For the example just discussed, they would also construct the S_p shown in Figure 10. However, their constructive technique would apply equally well to the concurrence

$$\Gamma = AB + AC$$

whose hypergraph representation is not disjoint so that our Theorem 1 would not apply. Since concurrence schemes are drawn from the power set of the set of n participants, the cardinality of Γ can be exponential in n , hence Ito, Saito and Nishizeki's construction is more in the nature of an existence proof (for perfect shared secret schemes) than a practical method of construction.

Theorem 2. The geometric realization for a concurrence scheme Γ in which Γ can be factored into the product of disjoint logical expressions is the space spanned by the disjoint geometrical realizations of the factors.

Theorem 2 can be applied to concurrence scheme 13 in Figure 5, which is one of those for which the reader was challenged earlier to construct a shared secret scheme:

$$\Gamma = ABC + AD = A(BC + D) \quad .$$

Applying Theorem 2, we easily construct one such shared secret scheme:

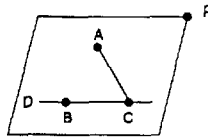


Figure 12.

Theorem 3. The geometric realization for a concurrence scheme in which Γ can be factored into the sum of the products of expressions disjointly partitioning the variables, can be realized as the union of geometric realizations of the form given by Theorems 1 and 2.

Theorem 3 can be applied to concurrence scheme 14 in Figure 5 (the second of the challenge schemes)

$$\Gamma = ABC + AD + BD = (AB)C + (A+B)D \quad .$$

One of the shared secret schemes that can be constructed using Theorem 3 is:

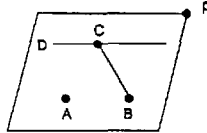


Figure 13.

Theorem 4. The concurrence scheme Γ whose hypergraph representation is $G_\Gamma = K_{k;\ell}$ (the complete hypergraph consisting of all $\binom{\ell}{k}$ k -edges on ℓ vertices) can be realized by a set of ℓ linearly independent points in a $(k-1)$ -dimensional indicator space.

Proof: Γ consists of all of the $\binom{\ell}{k}$ k element subsets of the ℓ participants, i.e., it is a simple (k, ℓ) threshold scheme. Given ℓ linearly independent points in a $(k-1)$ -dimensional space, no subset of j , $2 \leq j \leq k-1$, of the points can lie in a $(j-1)$ -dimensional subspace. Therefore, since V_i is only $(k-1)$ -dimensional, every subset of k of them must span V_i . ■

Theorem 4 can be applied to concurrences 11 and 19 in Figure 5. The construction of S_{11} (four collinear points) is obvious. The construction of S_{19} is somewhat more interesting, consisting in this special case ($n = 4$) of four points in general position in a plane, V_i , no pair of which are collinear with the indicated point p .

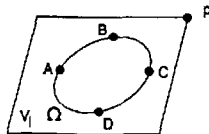


Figure 14.

The curve Ω lying on the four points A, B, C and D is a conic, i.e., for a field of odd characteristics a set of points in V_i no three of which are collinear. The same construction would hold for any $(3, \ell)$ threshold

scheme. The maximum value for l would be q if p lies on Ω and $(q+1)/2$ if it doesn't, since each secant of Ω through p can only lie on one point of Ω that can be used as a private piece of information.

Theorem 5. If in the hypergraph representing a concurrence scheme there are two or more independent and isomorphic points, all of these points can be identified in a reduced hypergraph representing the same concurrence scheme.

Theorem 5 is probably the most useful of all of the results given here. It applies to many of the concurrence schemes shown in Figure 5. We will use number 10 to illustrate its utility:

$$\Gamma = AB + AC + AD + BC + CD$$

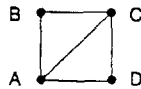


Figure 15.

Vertices B and D are independent and isomorphic, and hence by Theorem 5 can be identified. Consequently, Γ can be replaced by the simpler

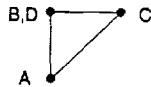


Figure 16.

to which Theorem 4 applies. One of the resulting shared secret schemes is:

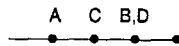


Figure 17.

Almost as useful as Theorem 5 itself, is the following Corollary which allows a designer to add new participants to an existing shared secret

scheme in those cases where the new participants are intended to have the same capability as one (or more) of the existing participants.

Corollary: Given a realization of a concurrence scheme, any share can be given to as many participants as desired—all of whom will be independent and have isomorphic capabilities.

Figure 18 shows a geometric shared secret scheme realizing each of the concurrence schemes shown in Figure 5. Some of these constructions are obvious a priori, others—constructed with the assistance of various of the theorems just given—are obvious after the fact, while a few may not be obvious at all.

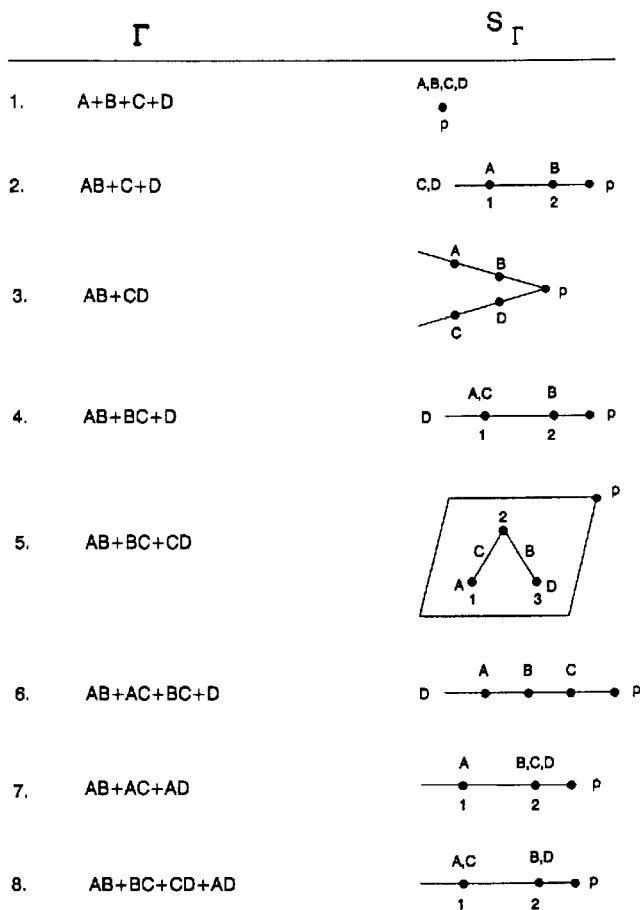


Figure 18.

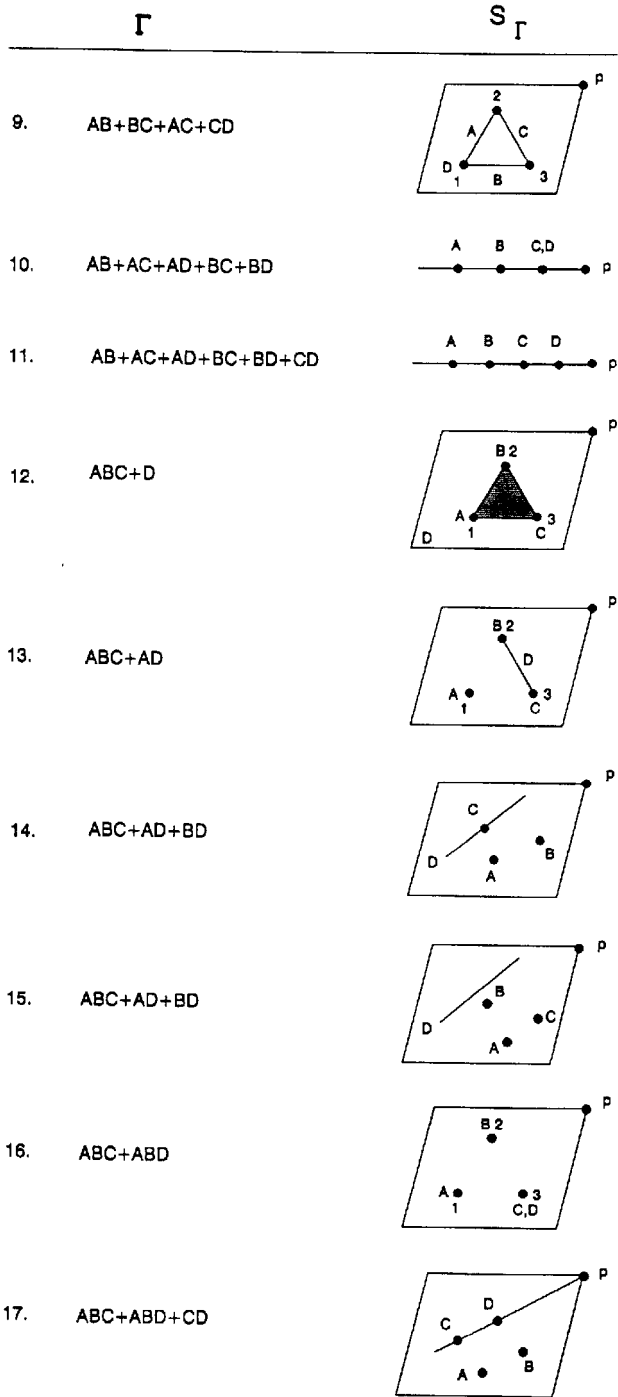


Figure 18. (cont'd)

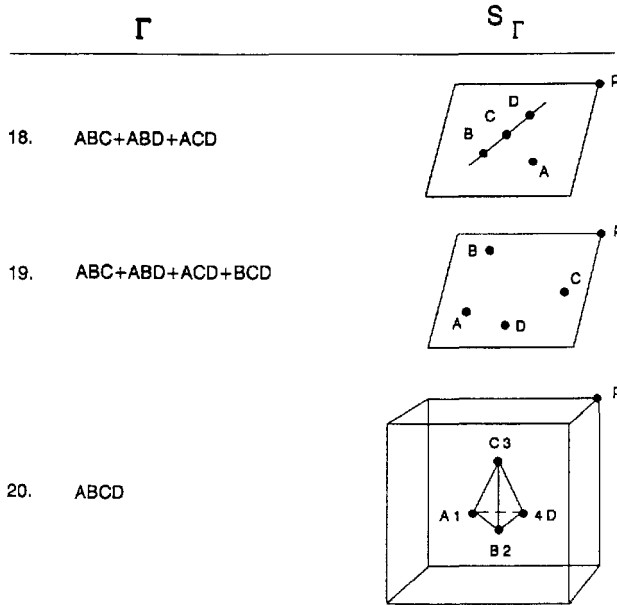


Figure 18. (cont'd)

The constructions for S_Γ given in Figures 6, 7 and 18 support (and prompt) the following conjecture.

Conjecture: Every monotone concurrence scheme can be realized by a perfect geometric shared secret scheme.

Remark: Ito, Saito and Nishizeki [6] proved that every concurrence scheme can be realized by a perfect shared secret scheme, as did Benaloh-Leichter [1] using a different technique. The conjecture is that for every concurrence scheme Γ , it is possible to choose a space V_i and a collection of subspaces of V_i that can be assigned to the participants to realize Γ in a geometric shared secret scheme.

The Consequences of Trust

Thus far in this paper, and without exception in the literature on shared secret and/or shared control schemes, it has been assumed that the participants will not divulge their private pieces of information—except perhaps at the time the controlled event is initiated. This is

not the same as assuming that the participants are unconditionally trustworthy, and in fact several persons have studied the problem of how to make the functioning of a shared control scheme be reliable when (some) participants may not be [2,3,4,5,7,8,9]. Realistically, though, one must accept the possibility that a participant may share what he knows with whomever he trusts. The consequences of such sharing may be surprising (to the key distribution center who set up the secret sharing scheme with a desired concurrence in mind). For example, in the two participant scheme to realize $\Gamma = AB$ (2 in Figure 3) if A trusts B and tells him his private piece of information, B can thereafter unilaterally initiate the controlled action. This isn't what the key distribution center had in mind, since it was his intention that A and B would have to concur at the time that the controlled event is to be initiated. However, there is no notion of simultaneity in the logic of shared control, only a specification of which private pieces of information will be needed to initiate the controlled action. In the example, A's input is required and is present—in B's possession. In effect, A has given B his proxy which B can exercise whenever he chooses. Thus, even though the resulting control is not what the key distribution center had in mind, it is also not a logical surprise either.

On the other hand, consider the concurrence scheme $\Gamma = AB + AC + AD$ (7 in Figures 5 and 8). The intent of the key distribution center in this case is that A must concur with at least one of B, C or D in order for the controlled event to be initiated. We have already discussed a similar example in the setting of a treaty controlled action where A (say the U.S.) retains a veto power over the action, but in spite of this absolute veto capability can't unilaterally initiate the controlled action. In the present example, this requires the concurrence of at least one of the three other signatories to the treaty. Now assume that A trusts B and C together and shares his private piece of information with them in such a way that they can jointly reconstruct his input to the shared control scheme. Neither B nor C alone can initiate the controlled action. The unexpected result though is that B, C and D together could then initiate the controlled action. Γ has been replaced with a new concurrence scheme

$$\Gamma' = AB + AC + AD + BCD$$

where the three participants B, C and D can act without needing A's concurrence. This consequence of A's trust of B and C is more surprising than the result in previous example, since there a proxy (trust relationship) was used to eliminate a participant from an authorized subset of Γ . Here it is used to replace a participant in an authorized concurrence with a subset of the other participants. The result is that new (and unexpected) sets are capable of initiating the controlled action. In both cases, a literal (A in both of these examples) is replaced with a trusted subset (BC). In the first case, a participant is eliminated as a result, while in the second, one participant is eliminated and two are added:

$$ABC \rightarrow BCBC \rightarrow BC \quad \text{and} \quad AD \rightarrow BCD \quad .$$

The basic notion (and problem) should be clear from these two small examples. If one or more of the participants trust some collections of the other participants, i.e., if they share their private pieces of information in such a way that subsets that they trust can jointly act in their stead the result may be that quite different concurrences than were originally intended (Γ) may be able to initiate the controlled action.

When a key distribution center sets up a shared control scheme S_{Γ} to realize a concurrence Γ , he must implicitly accept all of the concurrence schemes reachable from Γ as a result of the possible trust relationships between the participants—since he can't know and can't control who trusts whom. Incidentally, there are concurrences that are not reachable from a given concurrence; for example $\Gamma = AB$ is not reachable from $\Gamma = A + B$, since if both participants are initially able to unilaterally initiate the controlled action, nothing that can be done by either participant can lessen the other's capability. Since trust relationships can only increase the capability of groupings of participants, and can never take capability away from a subset C that previously had it ($C \in \Gamma$), a lattice of concurrence schemes can be defined, in which the nodes are concurrence schemes and the edges are trust relationships. At Crypto'90 in the lecture on which this paper is based we made a conjecture as to the structure of this lattice—essentially equating the lattice of concurrence schemes Γ and the geometric lattice of the hypergraph representations of these schemes G_{Γ} .

In the case of two participants, AB dominates A + B, and the trust relationship to reach A+B from AB is that A must trust B and vice versa. For three participants the situation is more complex. Obviously ABC dominates all other concurrence schemes and A+B+C is dominated by everything else. The ordering of the other three concurrence schemes however requires some analysis. AB+AC dominates AB+AC+BC since if A trusts B and C jointly (meaning that A can be replaced by BC), we have

$$AB + AC \rightarrow BCB + BCC \rightarrow BC$$

and

$$\Gamma' = AB + AC + BC$$

Similarly AB + AC + BC dominates AB+C, requiring that A trust C. Three participant concurrence schemes therefore are ordered as shown in Figure 19.

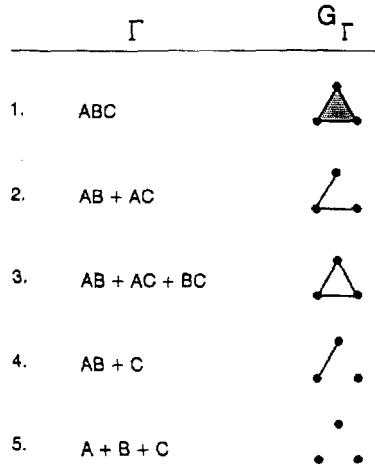


Figure 19.

The geometric lattice (of hypergraphs) in which order is determined by set (edge) inclusion has a different order however:

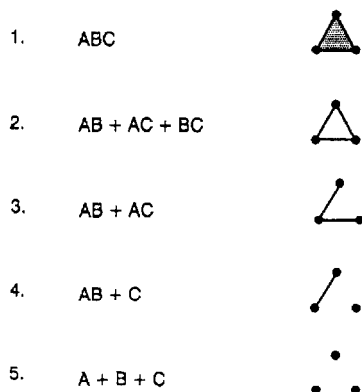


Figure 20.

The reversal of the order of $AB+AC+BC$ and $AB+AC$ in these two lattices is a counterexample to the equivalence of the geometric lattice and the lattice of concurrence schemes that had been conjectured. At the present, we are unable to even conjecture what the relationship between the two lattices may be. Figure 21 shows the geometric lattice for three participants. The lattice of concurrence schemes is still being investigated for even this small case. Instead of the (refuted) conjecture, we instead, ask the fundamental questions (for shared secret and/or shared control schemes).

Question 1. Given a shared secret scheme Γ what other shared secret schemes are reachable from Γ as a result of trust relationships that may exist among the participants.

The next question is closely related, but not necessarily the same.

Question 2. Characterize the lattice of concurrence schemes for n participants.

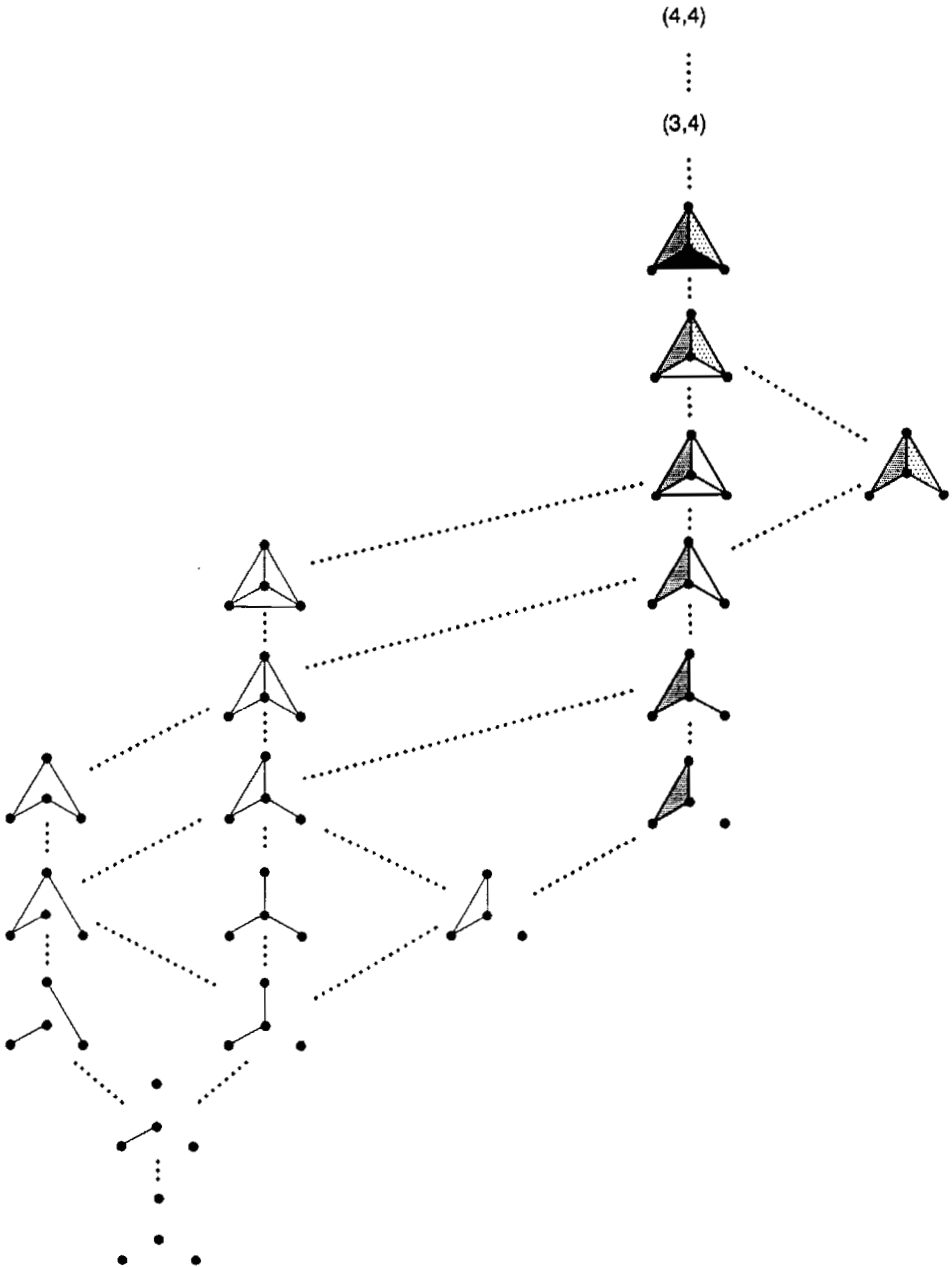


Figure 21.

The reason that we say that Questions 1 and 2 may not be equivalent is that it could be the case that concurrence scheme Γ_2 is reachable

from concurrence scheme Γ_1 , and Γ_3 from Γ_2 , but that there is no set of trust relationships that reach Γ_3 directly from Γ_1 .

The answers to both of these questions are of vital importance to the discipline of shared capability since a key distribution center setting up a shared control scheme Γ must—implicitly—accept every scheme reachable from Γ as well.

References

1. J. Benaloh and J. Leichter, "Generalized Secret Sharing and Monotone Functions," Crypto'88, Santa Barbara, CA, August 21-25, 1988, Advances in Cryptology, Ed. by G. Goos and J. Hartmanis, Vol. 403, Springer-Verlag, Berlin, 1990, pp. 27-35.
2. E. F. Brickell and D. R. Stinson, "The Detection of Cheaters in Threshold Schemes," Crypto'88, Santa Barbara, CA, August 21-25, 1988, Advances in Cryptology, Ed. by G. Goos and J. Hartmanis, Vol. 403, Springer-Verlag, Berlin, 1990, pp. 564-577.
3. B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults," Proc. 26th IEEE Symp. Found. Comp. Sci., Portland, OR, October 1985, pp. 383-395.
4. I. Ingemarsson and G. J. Simmons, "How Mutually Distrustful Parties Can Set Up a Mutually Trusted Shared Secret Scheme," International Association for Cryptologic Research (IACR) Newsletter, Vol. 7, No. 1, January 1990, pp. 4-7.
5. I. Ingemarsson and G. J. Simmons, "A Protocol to Set Up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party," to be presented at Eurocrypt'90, Aarhus, Denmark, May 21-24, 1990, Advances in Cryptology, to appear.
6. M. Ito, A. Saito and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," (in English) Proc. IEEE Global Telecommunications Conf., Globecom'87, Tokyo, Japan, 1987, IEEE Communications Soc. Press, Washington, D.C., 1987, pp. 99-102. Also to appear in Trans. IEICE Japan, Vol. J71-A, No. 8, 1988 (in Japanese).
7. G. J. Simmons, "Robust Shared Secret Schemes or 'How to be Sure You Have the Right Answer Even Though You Don't Know the Question'," 18th Annual Conference on Numerical Mathematics and Computing, Sept. 29-Oct. 1, 1988, Winnipeg, Manitoba, Canada, Congressus Numerantium, Vol. 68, May 1989, pp. 215-248.
8. G. J. Simmons, "Prepositioned Shared Secret and/or Shared Control Schemes," Eurocrypt'89, Houthalen, Belgium, April 11-13, 1989, Advances in Cryptology, to appear.

9. M. Tompa and H. Woll, "How to Share a Secret with Cheaters," Crypto'86, Santa Barbara, CA, Aug. 19-21, 1986, Advances in Cryptology, Vol. 263, Ed. by A. M. Odlyzko, Springer-Verlag, Berlin, 1986, pp. 261-265; also Journal of Cryptology, Vol. 1, No. 2, 1988, pp. 133-138.