Prepositioned Shared Secret and/or Shared Control Schemes[1]

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

Abstract

Secret sharing is simply a special form of key distribution.

Introduction

This is the third in a series of papers devoted to the analysis and realization of much extended capabilities for shared secret and/or shared control schemes over and above what can be achieved by simple (k,ℓ)-threshold schemes [42,43]. Since an essential first step has been to understand as clearly as possible the underlying principles on which shared control is based, all of the papers -- this one included -- have also been concerned with the formulation of a simple unifying model of sufficient generality to encompass all of the extensions.

The need for additional capabilities has thus far occurred in three main areas: in the enforcement of command objectives, either of the national command authority or of the subordinate military commands, in the implementation of multinational controls of treaty controlled actions and as described in other sources, in meeting the needs of the financial and banking community. In both military command and in banking applications, there is frequently a requirement for the control scheme to accommodate more than one class of participants with differing capability to initiate the controlled action. While it is certainly true that no two members of the Joint Chiefs of Staff equal the President (in terms of their command authority), one can easily conceive of circumstances in which the President might wish to prearrange for them to be able to act in his stead. For example, the President anticipating circumstances under which he would be unable to act might wish to give an order of the form: "If two of you agree that this circumstance has occurred, then this is what you should do..." -- the gravity of the action being so great that he wants to be certain that at least two of them concur before the action can be initiated. Similarly, in military command schemes, there is a frequent need to make the command structure be less vulnerable to a decapitation type attack, which can be achieved by making it possible for lower levels of command under some circumstances to autonomously initiate actions that normally could only be initiated by higher echelons of command. In most instances, the only acceptable way this can be done is to compen-

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

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 436-467, 1990.

sate for the lower level of authority (and hence of responsibility) by requiring a higher level of concurrence before the action can be initiated. This could be done by implementing separate and independent simple k_i-out-of-ℓ_i threshold schemes for each level of command (control). However, in almost all such multilevel control schemes it is required that capability be hereditary, meaning that any member of a higher level of capability class should be able to function as a member of a lower (less capable) class, with the diminished capability of a member of that class. In other words, if the concurrence of any two colonels, or of any three majors, suffices to reconstitute the launch enable code for a tactical missile, then it is inconceivable that one colonel and two majors acting together should not also be able to launch the missiles. Precisely the same situation arises in a banking setting in which any two vice presidents or any three senior tellers can authenticate an electronic funds transfer. In such a scheme, any vice president along with any pair of senior tellers should be able to do so also.

In the case of treaty controlled actions, irrespective of whether the controlled action is the direct object of the treaty or only associated with verifying compliance with the conditions of the treaty, there are at least two parties with differing, and oftentimes competing, objectives. In the simplest situation of this type, two parties have agreed that it should be impossible to initiate an action unless they both agree. At the place (or time) at which the control is effected, each party has its own control team to insure that their national input to the control scheme will only be made under the agreed upon circumstances. The type of concurrence each nation requires of its control team members in order for their national input to be made can vary widely. In analogy to the U.S. practice of the two-man control of nuclear weapons (and associated enabling information) or of the launch control of strategic missiles, a national control team could consist of two members, neither of whom has the capability to act alone, but who can jointly make their nation's input to the control scheme. It could equally well be a multilevel control scheme of the sort discussed in the preceding paragraphs. The important point is that in these control schemes there are two or more parties, none of whom can substitute for any of the others.

The first paper in this trilogy, "How to Really Share a Secret" [42] was devoted to these two extensions to threshold schemes: multilevel and multipart(y) control schemes. Only later did we realize that these were simply special cases of a single category of extended capability; namely, general concurrence schemes. In the most general formulation of concurrence schemes, there is a set of participants (the insiders) each of whom has a piece of private information related to a secret piece of information, not all of which is known to any other participant nor to any outsider. A concurrence scheme specifies those subsets of the participants that are supposed to be able to recover the secret or to initiate the controlled action by pooling their private pieces of information. Simple threshold schemes or even

multilevel and/or multiparty schemes are distinguished only in that in these cases there is a concise way of describing the authorized subsets of participants. Ideally, any subset of the participants that doesn't include one of the authorized groupings should have no better chance of recovering the secret than does an outsider. Schemes that satisfy this condition have been called perfect by Schellenberg and Stinson [40], a terminology we will adopt here also. Clearly in a perfect shared control scheme the information content of the part of each participant's private piece of information that he must keep secret is at least as great as the information content of the secret information itself. If there were any participant for which this wasn't true, then an unauthorized subset of the participants which could be made into an authorized subset by having the participant in question join with them would have less uncertainty about the secret than an outsider: contradicting the assumption that the scheme is perfect. This quantity of information is commonly referred to as a share. All of the extended capability schemes described in [42], i.e., multilevel and multiparty schemes and simple combinations of these, are characterized by each participant only having to keep secret a single share of information. Shared secret schemes of this sort are said to be ideal. At Crypto'88, Benaloh showed that there were concurrence schemes which could not be realized by any ideal scheme [3]. The paper by Brickell "Some Ideal Secret Sharing Schemes" [19] addresses the question of characterizing ideal shared secret schemes in general. Although generalized concurrence is not the subject of this paper, a brief Appendix to this paper concludes our treatment of multilevel and multipart shared secret schemes begun in [42]. The point to the remarks of the last several pages is that one direction of generalization for shared secret and/or shared capability schemes is to be able to realize much more general concurrences than unanimity or simple k-out-of-ℓ threshold schemes.

In most applications for shared control schemes, the consequences of an authorized concurrence are immediate. For example, if two vice presidents of a bank must enter their private pieces of information into the locking mechanism of the vault in order for the secret combination to be reconstituted and for the door to open, they know immediately whether their action has been successful or not since the vault door either opens or else remains shut and locked. Similarly, the missile launch control officers also have an immediate confirmation of the correctness of their inputs if the missile is launched. The second paper of this trilogy, "Robust Shared Secret Schemes or 'How to be Sure You Have the Right Answer Even Though You Don't Know the Question'" [43], was devoted to the problems that arise if the consequences of a shared control scheme are distant in either time or place from where the private pieces of information are input. If the shared secret scheme controls the enabling of a missile warhead, it is clearly desirable to know that the warhead has not been enabled prior to launch as opposed to learning that it wasn't after its arrival over the target. In this application, it would be easy enough to provide a

simple go/no-go indication of status, but there are applications in which this isn't feasible. Perhaps the most convincing example is provided by a scheme to accomplish the remote activation/deactivation of preemplaced smart mines. Conceivably it would be possible to have the mines report their status on request, but this could give away their location to an opponent passively eavesdropping on the communication. On the other hand, the information needed to deactivate the mines is at least as important (militarily) as the effort required to locate and destroy them, which justifies its shared control. In this case the action (the mine's function) is distant in both time and place from the point from which they are controlled so it is vitally important for the host nation to know that the mines have indeed been turned off before he runs a convoy through the field, and equally important that he know that they have been reactivated after the convoy's passage.

Basically, this class of problems is analogous to the collection of communications problems addressed by error detecting and correcting codes, the most obvious difference being that the signal is tested for correctness on receipt in the one case and prior to transmission in the other. In the application to shared control schemes, we want to be able to verify (in probability) that the correct secret value has been reconstructed (error detection) and, if it hasn't, to be able to recover from the error (error correction). Since there are many applications for shared control schemes in which the controlled action is distant in either time or place or both from the place at which the control is effected -- such as the enabling or turn-off of space-based defense systems, self-destruct commands to aberrant missiles and/or space shots, the activation and deactivation control of smart mines as described above, etc.; the second area of extended capability for shared control schemes has to do with providing means to verify whether the correct value for the secret has been reconstructed and, if not, to recover from the error. In "Robust Shared Secret Schemes," a general technique was described that makes it possible for the participants to verify (in probability) whether they have reconstituted the correct value for the secret information, even though they have no way of knowing either before or after the fact what the secret value is.

In this paper, we consider a third class of extended capabilities to shared control schemes that are difficult to describe separated from a detailed description of the implementation of the schemes. Roughly speaking, in the applications of interest here we wish to separate the private pieces of information, whose function it is to reveal a secret piece of information under appropriate circumstances, from the secret piece of information they conceal. This almost sounds paradoxical; however, the need for such a capability arises in several real-world applications for shared control schemes.

We mentioned earlier in connection with a description of multilevel concurrence schemes the problem of a decapitation attack on command. Although this terminology is suggestive, it may not be self-explanatory. If there is information which is

held by a higher level of command that must be communicated to lower levels of command in order for some action to be initiated -- such as arming warheads, launching missiles, etc. -- an adversary may attempt to prevent the action from occurring by destroying the higher command in a surprise attack before the information can be disseminated to the lower levels of command. This is called a decapitation attack. There is another aspect to decapitation attacks in that if the higher levels of command are destroyed, the lower levels may either not know what to do or else be ineffectual in their response. We are not concerned with these consequences to a decapitation attack, though, but only with the situation in which the lower levels of command are rendered incapable of carrying out an action, that they are otherwise able to do, because one or more pieces of information needed to initiate the action were prevented from reaching them by the attack on the superior command. Multilevel shared control schemes were devised specifically to solve this problem in situations in which the lower level of authority (and hence responsibility) at a lower level of command could be satisfactorily compensated for by requiring an increased level of concurrence for the action to be initiated. There are actions, however, in which either the law doesn't permit a delegation of authority (and hence capability) irrespective of the concurrence that might be required for it to be exercised, or else in which the party(ies) holding the capability are not willing to delegate the capability under normal circumstances. The crucial words in this description are "under normal circumstances" implying that there are circumstances that would either permit such a delegation to be made or in which such a delegation would be acceptable. The problem, from the standpoint of the shared secret or shared control scheme, is the same in either case.

Consider a missile battery at which there are a dozen officers. The consequences of a missile being launched without proper authority would be so great that in normal times (peacetime or in lower levels of alert) the capability to initiate such an action is to be held at a higher level of command: in other words, the policy is that even if all of the officers at the battery believe that a missile should be launched, they should not be able to do so without requesting authorization from the superior commander (and more importantly, could not do so without being given the launch enable codes). In the absence of a shared control scheme, the only way that the superior commander could protect against a decapitation attack on his headquarters (and him) would be to preemptively enable the missiles as a part of going to an advanced state of alert. But these are precisely the circumstances in which there is the greatest concern that something might go wrong and a missile be launched when it shouldn't have been. Requiring the concurrence of k of the battery officers, say two of them, for a launch is a way of increasing confidence in the proper execution of the plan of battle. What is needed is a scheme in which, under normal circumstances, only the superior commander has the capability to enable a missile launch, but which would allow him, when intelligence inputs or other early

warnings indicate, to delegate a 2-out-of-12 shared control of the launch to the battery to prevent a decapitation attack from succeeding. The problem is: How does he establish the 2-out-of-12 shared control scheme at the time the battery goes to an advanced state of alert? If no advance arrangements have been made, the twelve pieces of private information would have to be communicated to the battery officers in a secure and authenticated manner, at a time (advanced stage of alert) when communications are apt to be both congested and disrupted. Even if the information could be communicated to the battery at that time, the risk of human error in dealing with unfamiliar codes of a size at the limits of mnemonic aids to memorization would be high. Ideally, it should be possible to distribute the private pieces of information in advance of a need to use the shared control scheme, but with the constraint that in normal circumstances even if all of the participants were to violate their trust and pool their private pieces of information they would still have no better chance of recovering the secret than an outsider would have of simply guessing it. In such a scheme, at the time the battery is put in an advanced state of alert, a single piece of information (one share in the terminology introduced earlier) would need to be communicated by the superior commander to activate the prepositioned 2-out-of-12 shared control scheme so that any two of the officers would thereafter be able to launch the missiles. The important point to this discussion is that almost all of the information needed to implement the shared control (the private pieces of information) could be communicated in advance of the need during a time of low tension and reliable communications. Since there is no special urgency during this set-up phase, the communication could even be handled by courier or by having the officers in the subordinate command come to headquarters to be given their private pieces of information. At a time when the battery is going to a state of advanced alert, i.e., a period of high tension when communications will be at a premium, only a single share (the minimum amount) of information needs to be communicated to activate the scheme.

This same example (a missile battery) can also be used to illustrate the other extended capability to shared control schemes which is also the subject of this paper. There are two ways this need can arise. First, consider the case in which not all of the missiles have the same launch enable code. The problem in this case is to devise a scheme which can be prepositioned that will allow any one, or any selected subset, of the launch enable codes to be activated in a shared control scheme without affecting the quality of control of the unreleased missiles. Clearly, this could be accomplished by prepositioning a shared control scheme for each launch enable code, almost equally clearly this would be a completely unacceptable solution since each participant would be required to remember several private pieces of information, each of which is near the limit of even mnemonically aided recall. What is needed is a way that the same pieces of private information can be used to recover different pieces of secret information.

Another equally important problem has to do with how the battery can stand down from an advanced state of alert, where standing down means reverting to the kind of control that existed prior to the alert. In order for this to be possible, the scheme must provide both a capability for the superior commander to activate the shared control scheme (delegate authority) and to deactivate it, i.e., to rescind his delegation of authority, if the circumstances change so that an advanced state of alert is no longer warranted. If the system is to truly revert to the same type and quality of control after a recall that it had prior to the alert without changing the private pieces of information involved in the shared control scheme, then both the activating information which is to be sent by the superior commander and the enabling code that the missile will respond to must change with each delegation of authority, irrespective of whether the delegated capability was exercised or not. Although it is inappropriate to the purpose of this paper to say much about the practical problems of implementing shared control schemes, it is perhaps worthwhile remarking that there are two ways (at least) to achieve this. The simplest scheme would be for the enable codes to change automatically as a function of time; say once each day. Another approach would be for the mechanism in the missile controller that carries out the calculation of the secret information from the private pieces of information to have a stored list of enabling values, only one of which would be operational at a time. In a scheme of this type, the activating piece of information that is sent by the superior commander would have to correspond to the current value of the secret if the shared control is to be operable. If a recall is received (from the superior command), its entry would advance the store to the next stored value for the secret and output a piece of information that could only be obtained by executing this protocol. This would return the missile to a condition wherein only the superior commander could enable it for a launch, or delegate its release if the battery was later put in an advanced state of alert again. The old value of the secret information would become invalid so that stale values of the activating information would not be operable. The unique output which could only be obtained by properly carrying out the recall protocol could be returned to the superior command to verify that the control system had been returned to its prealert status.

The point of this lengthy discussion of the simple, but plausible, example of a missile battery was to illustrate as clearly as possible the two essential features to the schemes that are the subject of this paper:

a) It should be possible to preposition all of the private information needed for the shared control subject to the condition that even if all of the participants were to violate the trust of their position and collaborate with each other, they would have no better chance of recovering the secret information than an outsider has of guessing it.

b) It should be possible to activate the shared control scheme once it is in place by communicating a single share of information, and for many applica-

tions, it should also be possible to reveal different secrets (using the same prepositioned private pieces of information) by communicating different activating shares of information.

There are numerous applications that require these capabilities of shared control schemes, however, we will not discuss the details of these applications further but concentrate instead on a discussion of how such extended capabilities can be achieved. Since this depends critically on the implementation of the shared control schemes, we must first digress to describe the general model for shared control schemes.

General Model for Shared Secret and/or Shared Control Schemes

There are two essentially different ways in which pieces of information related to another, secret, piece of information can be constructed and distributed among a group of participants so that designated subsets of the participants can recover the secret piece of information, while no collection of participants that doesn't include one of these subsets can. One of these classes of shared secret schemes can be adapted to provide the extended capabilities that are the subject of this paper, while the other cannot. We begin our development of the general model with a discussion designed to clarify the essential difference between the two classes of schemes.

In some schemes, the set of possible values for the secret, consistent with all of the private pieces of information that have been exposed, remains unchanged until the last required piece of private information becomes available, at which point the unique value for the secret suddenly becomes the only possibility. In others, as each successive piece of the private information is exposed, the range of possible values that the secret could assume narrows, until finally when the last required piece of private information becomes available, the secret will have been isolated and identified. There are numerous examples of each type of system. It is easiest to illustrate this behavior using a pair of small examples.

First, consider the simplest possible example of a shared secret scheme, a 2-out-of-ℓ scheme:

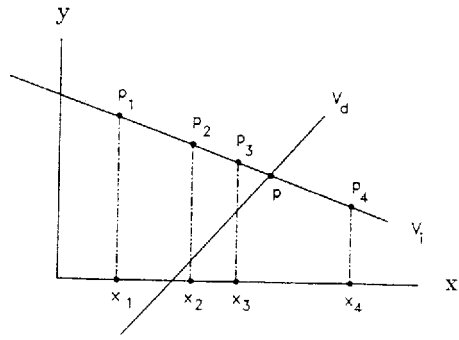


Figure 1.

The private pieces of information are points on a line V_i, whose intersection with a line V_d is the index point, p, at which the shared secret information is defined: $p = (x_p, y_p)$. As was pointed out in "How to (Really) Share a Secret" [42], the information needed to specify one of the points, p_i, is not all of the same type insofar as its security requirements are concerned. If we use the obvious specification of the point p_i in the affine plane AG(2,q) by its coordinates (x_i, y_i), then it is sufficient (for the security of the shared secret scheme in this example) that each participant keep secret one of the coordinate values (say y_i), and that he merely insure the integrity of the other coordinate value against substitution, modifications, etc. With this convention for partitioning the private pieces of information into secret and nonsecret parts, V_i cannot be parallel to the y axis since in that case $x_i = x_p$ for all i and V_i could be deduced from the exposed (nonsecret) parts of any pair of the private pieces of information.

The point we wish to make using this simple scheme has to do with the probability of some improper (i.e., unauthorized) collection of persons recovering the secret. An outsider who knows only the public parts of the private pieces of information, but none of the secret parts and the geometrical nature of the scheme, i.e., the line V_d and that there is a line V_i whose intersection with V_d determines the unknown point p, cannot restrict the possible values for p beyond the fact that it is on V_d. Since each of the q points of V_d has the same number of lines on it that are not parallel to the y axis and hence which could be the unknown line V_i, it should be obvious that the opponent can be held to an uncertainty about the secret of

$$H(p) = \log(q) \quad , \tag{1}$$

i.e., his "guessing probability" of choosing p in a random drawing using a uniform probability distribution on the points of V_d.

Now consider the uncertainty faced by one of the participants; an insider. He knows his private piece of information, the point p_i on V_i, the public abscissas x_j, $j \neq i$, for the other participant's private pieces of information and the line V_d. Each point, p', on V_d determines a unique line lying on both p' and p_i which could be the unknown (to the participant) line V_i. Clearly, his uncertainty about the secret is the same as that of an outsider who has no access to any privileged information

$$H(p) = \log(q) \quad . \tag{2}$$

These are the only two meaningful improper groupings of persons in this example since no combination of outsiders with an insider is more capable (in improperly recovering the secret) that is the insider alone. Consequently, this is a perfect 2-out-of-ℓ scheme.

We next consider another 2-out-of-ℓ shared secret scheme:

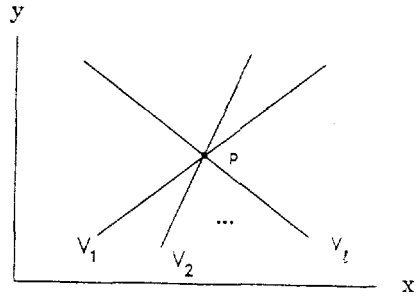


Figure 2.

In this case, the private pieces of information are lines all of which are concurrent on the secret point p. To an outsider, every point in the plane is equally likely to be the point p, hence his uncertainty about p is

$$H(p) = \log(q^2) = 2\log(q) \quad . \tag{3}$$

An insider, on the other hand, knows that p must be a point on the line which is his private piece of information. Hence, his uncertainty is only

$$H(p) = \log(q) \quad . \tag{4}$$

Consequently, this scheme is not perfect, since the insiders have an advantage (in cheating) over an outsider. Both schemes, however, provide the same minimum level of security against unauthorized recovery of the secret information. From that standpoint alone, they would appear to be equally good. There are other factors that need to be considered, such as the amount of secret information each participant must be responsible for -- or even the information content of the part whose integrity must be insured -- and the information content of the secret itself. Since the plane is 2-dimensional in both points and lines, it is easy to see that in either example the participant need only keep the equivalent of one coordinate value, i.e., $\log_2(q)$ bits, secret about his private piece of information and to insure the integrity of a like amount of information. Thus, the two schemes are equivalent with respect to these parameters. It is at least plausible to define the information content of the secret to be the least uncertainty faced by any unauthorized person or grouping of persons about it; in other words, $\log_2(q)$ bits in both examples as well.

The bottom line to this discussion of the two small examples is that while they are certainly different (not just superficially in the geometrical implementations) they are also alike in important respects. It is the differences that we wish to understand in order to better understand shared secret schemes.

In the first example, where the secret was defined at the point p on the line V_d, the security of the scheme was measured by the uncertainty about p, which, as we saw, was the same for an outsider or for any one insider. We now examine this example from a different standpoint. Although it may seem strange at first to do so, the line V_i can be thought of as being a cryptographic key which encrypts the plaintext (ordinate) of a private piece of information into the ciphertext (abscissa). This is consistent with our convention that the ordinate is the information being protected (kept secret) and that the abscissa can be exposed. In this case, the secret information is the decryption of a known cipher text (the ordinate, x_p, of the point p) using the key V_i. If V_i is to define a cryptotransformation, it must not be parallel to either the y axis or the x axis in order for it to define a one-to-one mapping (i.e., a nonsingular linear transformation) of the y axis onto the x axis.

While it is essential for the simple shared secret scheme described here, that V_i be restricted to not be parallel to the y axis -- since as we explained earlier the exposed parts of the private pieces of information would reveal V_i in that case -- it isn't necessary that V_i be resticted to not be parallel to the x axis as well. If V_i is parallel to the x axis, then the secret coordinate of the point p would satisfy $y_p = y_i$ for all i, but this could only be discovered if two or more of the participants compared (exposed) their secret pieces of information. But in this example, any two participants have been assumed to have the capability to reveal the secret, not just to recover V_i. Therefore, there is no necessity to exclude lines parallel to the y axis in this example since we are only using the one-way nature of the encryption operation without any requirement that it also be invertible -- which will be satisfied so long as to each choice of a plaintext y_p, every ciphertext is an equally likely preimage.

Looked at in this way, we can calculate the uncertainty about the (secret) key to the various combinations of individuals. An outsider knows only that V_i is a line in the plane not parallel to the y axis, i.e., one of the q^2+q lines in the plane less the q lines parallel to the y axis, or q^2 lines in all. Hence his uncertainty about the key is

$$H(V_i) = \log(q^2) = 2\log(q) \tag{5}$$

which is twice his uncertainty about y_p, the encrypted value of the ordinate of p. Note that in this interpretation V_d has effectively been restricted to be the line parallel to the y axis lying on x_p. It should be noted that the outsiders' uncertainty about p, H(p), in the first example is the same as his uncertainty about V_i, $H(V_i)$ in this example.

There are q+1 lines through each point on the line V_d, one of which is V_d itself, and hence not a candidate to be the key V_i. Therefore the q^2 potential keys (lines in AG(2,q) not parallel to the y axis) are uniformly distributed q at a time on each of the q points of V_d; hence

$$H(p) = \log(q) \quad . \tag{6}$$

In other words, since the set of q^2 lines that could be the unknown key, V_i, are uniformly distributed on the points on V_d (q on each point) and are all equally likely to be the key, an opponent's chance of determining the secret by "guessing" at the value of the key is exactly the same as his chance of "guessing" the value of the secret in the first place: log(q) in either case.

Next consider the situation with an insider. He knows a point on the unknown key, V_i. There are q+1 lines through this point, q of which are potential keys. Consequently, there is a one-to-one association between the potential keys (given his insider information) and the possible values for the secret cipher. Thus for the insider

$$H(V_i) = H(p) = \log(q) \quad . \tag{7}$$

The point is that in the first example it was the uncertainty about the key that was eroded with the exposure of successive pieces of the private information, i.e., of plaintext/ciphertext pairs in the present setting, (only one such pair is possible in this small example; we are anticipating the general case in this remark), however the uncertainty about the secret index point, H(p) or more precisely $H(y_p)$, remains the same for any grouping other than one able to uniquely identify the key. So long as the surviving candidate keys uniformly map each plaintext into all possible ciphers, the uncertainty about the secret plaintext remains the same, even though the uncertainty about the key decreases with each successive piece of private information that becomes available. The second example has no intermediate key, so it is the uncertainty about the secret point, p, that is directly eroded by the exposure of successive pieces of private information. When viewed in this way, a very close relationship exists between cryptanalysis in depth (with the key as the depth component) and shared secret schemes.

The entire purpose of this discussion was to support the following conclusion: the information contained in each of the private pieces of information constrains the values that some other variable can take. If this variable is the secret, then the shared secret system cannot be perfect, since in that case, unauthorized groupings of insiders would necessarily have an advantage over outsiders in guessing at the value of the secret. If, however, the variable is an intermediate function, out of a family of functions, satisfying suitable constraints such as being entropy preserving over the space in which the secret is located, then the scheme can be perfect. Although we won't make direct use of the principle here, we are in fact faced with the problem of devising cryptosystems with the unusual property that they are immune to cryptanalysis in depth (against the key as the depth component) for all "improper" groupings of plaintext/ciphertext pairs, but cryptanalyzable with certainty of success in recovering the key given any set of plaintext/ciphertext pairs that includes at least one of the prescribed concurrences.

The example shown in Figure 1 contains all of the essential features for the general model we will use for shared control schemes, irrespective of how complex the required concurrence may be. Essentially there is one geometric object (an algebraic variety -- generally a linear subspace in some higher dimensional space), which can be determined given any subset of the points in it that includes at least one of the specified concurrence groupings, which intersects another object in a single point, p, at which the secret is defined. While p is a point in both of the sets, the lines V_i and V_d in the example, the first set is always secret (until it is reconstructed by an authorized concurrence among the participants) while in many applications the other is publicly known, a priori. We therefore refer to the geometric object (set of points) whose determination isn't shared amongst the participants as the domain variety, V_d, since the secret (argument) can be thought of as being a point concealed in its domain. The object determined by the shared information can be thought of as indicating (in the sense of pointing to) the secret point p in V_d. We therefore call this object the indicator (variety), V_i. A single shared secret scheme may have either several indicators, or several domains, depending on the nature of the concurrence that is being realized. In the example of Figure 1, the indicator was the line V_i, determined by any pair of the points on it. V_i could have been equally well replaced by a quadratic curve (determined by any three of its points) or a cubic (determined by any four of its points not lying on a quadratic curve, i.e., of rank four), etc. This, in fact, is the implementation of the shared secret scheme originally proposed by Shamir [41]. In this paper, we will only consider cases in which both V_i and V_d are linear subspaces of some higher dimensional containing space, $\mathbf{S}$. For most applications, $\mathbf{S}$ would be a projective space PG(n,q) over some field GF(q), however, all of our examples in this paper will be constructed in affine spaces AG(n,q), mainly because of the closer analogy to the more familiar Euclidean spaces. Our constructions make essential use of a simple result in projective geometry known as the rank formula:

$$r(U) + r(V) = r(U \cap V) + r(U \cup V) \tag{8}$$

true for all subspaces U and V of the containing space $\mathbf{S} = PG(n,q)$. r(x) denotes the rank of the subspace x. Note that r(x) = dim(x) + 1, and that the empty subspace has rank 0, and consequently dimension -1. It is easy to see that (8) does not hold in affine spaces. In AG(3,q) there are pairs of parallel lines, i.e., pairs of lines which do not intersect, but whose union is only a plane: $r(U \cap V) = 0$ and $r(U \cap V) = 3$ so that

$$r(U) + r(V) = 2 + 2 \neq 0 + 3 = r(U \cap V) + r(U \cup V) \quad .$$

From the standpoint of geometric intuition (8) is more accessible if rank is replaced by dimension:

$$\dim(U) + \dim(V) = \dim(U \cap V) + \dim(U \cup V) \quad . \qquad (8')$$

We are only interested in cases in which $V_i \cap V_d = p$, p a point, i.e., in which $\dim(V_i \cap V_d) = 0$. The following example, which we will make extensive use of, indicates the usefulness of (8'). In a 4-dimensional space, **S**, any pair of planes that do not lie in a common 3-dimensional subspace, intersect in a single point. Since they do not lie in a common 3-dimensional subspace, the $\dim(U \cup V) = 4$, so that we have

$$\dim(U \cap V) = \dim(U \cup V) - \dim(U) - \dim(U) = 4 - 2 - 2 = 0 \quad ,$$

hence, $U \cap V = p$, p a point. We will represent this 4-dimensional construction with the figure:

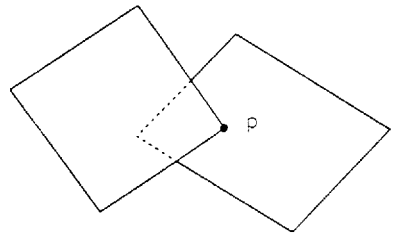


Figure 3.

Similarly, we will represent the intersection of a 3-dimensional subspace (of a 4-dimensional space **S**) with a line by the figure:

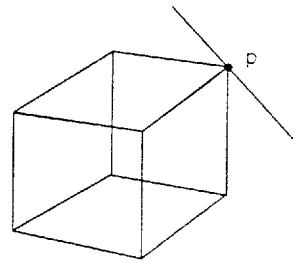


Figure 4.

Although the method of construction is completely general and independent of the dimensionality of the containing space **S**, all of the examples in this paper will be constructed using only the four lowest dimensional configurations:

S	U	V
plane	line	line
3-space	line	plane
4-space	line	3-space
4-space	plane	plane

In the Appendix to this paper, we analyze several shared control schemes that can be realized even within these small examples. The detailed discussion has been relegated to the Appendix so as to not interfere with the main line of development in the paper: devising prepositioned schemes that must await an activating piece of information before they become operational. There is one point in connection with those examples, though, that must be made here; namely, the concept of dual configurations. In Figure 1, both V_i and V_d were lines, and hence in some sense, indistinguishable. In other words, given two lines that intersect at the desired point, p, in the plane, it is immaterial which line is chosen to provide the concealment for p, V_d, and which is chosen to be shared, V_i. Similarly, in Figure 3 it is immaterial which of the planes is identified as V_d and which as V_i. In a sense, both of these constructions are self-dual in the sense that interchanging the role of the two varieties involved doesn't affect the control or security characteristics of the scheme. The construction shown in Figure 4, however, is different. If V_i is the line, then the only control scheme that can be realized is a 2-out-of-ℓ one to indicate a point in a 3-dimensional subspace. If, however, V_i is chosen to be the 3-space pointing to a point on the line, V_d, the situation is dramatically different. We won't even attempt an exhaustive listing of all of the possibilities in this case, but some of the shared control schemes that can be realized are:

Table 1.

1.	Simple threshold:	4-out-of-ℓ
2.	Two levels:	4-out-of-ℓ and 3-out-of-ℓ
	or	4-out-of-ℓ and 2-out-of-ℓ
3.	Three levels:	4-out-of-ℓ, 3-out-of-ℓ and 2-out-of-ℓ
4.	Two parts:	each part a 2-out-of-ℓ scheme. Both parts must concur, but neither can act in the stead of the other.
5.	$\geq$ 2 parts:	each part a 2-out-of-ℓ scheme. Two of the parts must concur.
6.	Three parts:	4-out-of-ℓ where the concurrence must include at least one member from each part.
	Etc.	

Clearly there is an enormous difference, in terms of the kinds of control that can be realized, depending on whether V_i is chosen to be the line or the 3-space in the configuration shown in Figure 4. If the dimension of the containing space, S, is even, there will always be a self-dual geometric configuration as we've already seen for the cases n = 2 and 4 in Figures 1 and 4, respectively. All other configurations have dual interpretations depending on which subspace is chosen to be the indicator: i.e., the line or the plane when dim(S) = 3 or the line or the 3-space when dim(S) = 4 as indicated in Figure 4. These small configurations suffice to permit us to illustrate (in the Appendix) all of the essential details of multilevel and multipart shared control.

Returning now to the discussion of shared control schemes given in the first part of this paper where we argued that in a perfect scheme it had to be the "key" that was revealed when an authorized concurrence of participants occurred. In the example used there, the dimension of the space, S, was only two and the configuration was self-dual both of which obscured several important points. We remarked that the plane was 2-dimensional in either points or lines, so that the uncertainty about the key was 2-dimensional to an outsider (2 log(q)) and 1-dimensional to an insider, but that the uncertainty about the secret was only 1-dimensional to either of them. These notions need to be generalized to arbitrary varieties. Stripped of the inessential (to the present discussion) details of how sets of points can be chosen in a variety V_i so that any of the designated subsets of them will suffice to reconstruct all of V_i, the configurations of interest are of the form:

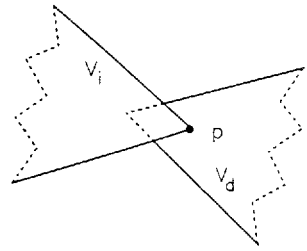


Figure 5.

where $\dim(V_i) + \dim(V_d) = \dim(S)$ and $\dim(V_i \cap V_d) = 0$.

Consider now the simple case in which $\dim(S) = 3$ and $\dim(V_i) = 1$, implying that $\dim(V_d) = 2$.

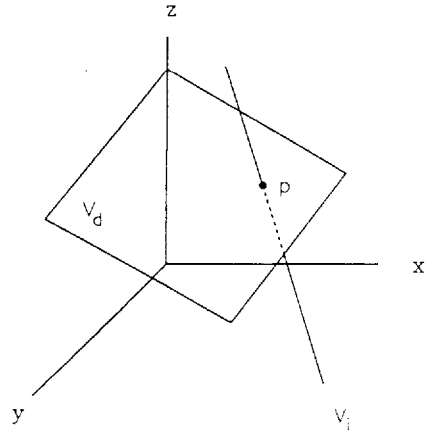


Figure 6.

In AG(n,q), there are q^n points, so there are q^2 possible values for p -- given that V_d is known a priori. On the other hand, the total number of lines in AG(3,q) is $q^2(q^2+q+1)$ of which q^4 have a single point in common with V_d, and hence are candi-

dates to be the unknown key. q^2 of these lines lie on each of the q^2 points in V_d. Similarly, considering the case in which one of the insiders is attempting to cheat, or in which one of the insiders' private piece of information has been exposed, there are q^2+q+1 lines through the point, q^2 of which have a single point in common with V_d, and hence are candidates to be the unknown key. One of these lines lies on each point in V_d, so that the uncertainty about the key is the same as the uncertainty about the secret, $H(V_i) = H(p) = \log(q)$, in this case.

In the first example, Figure 1, we saw the uncertainty about the key go from $O(q^2)$ to $O(q)$ to 1 as the concurrence progressed from an outsider to a single insider and finally to an authorized concurrence. Similarly, in the example just analyzed, we saw that the uncertainty about the key went from $O(q^4)$ to $O(q^2)$ to 1 for the same progression of concurrences. Since both examples were of 2-out-of-ℓ threshold schemes, the only difference is in the dimension of the subspace in which the secret point p is concealed: one in the first example and two in the second. As we shall see, this is no coincidence.

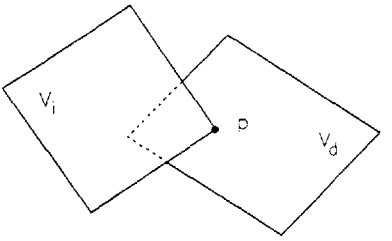


Figure 7.

Consider the self-dual construction shown in Figure 7 in which $\dim(S) = 4$ and $\dim(V_i) = \dim(V_2) = 2$. In AG(4,q), there are $q^2(q^2+1)(q^2+q+1)$ planes. $(q^2+1)(q^2+q+1)$ of these planes pass through each point, but if we assume that the point is known to be in one of the planes (either V_i or V_d by duality) then the number of planes that intersect it only at that point is only q^4. This is easy to see since there are $(q^2+1)(q^2+q+1) = q^4+q^3+2q^2+q+1$ planes on the point in all, one of which is the containing plane (V_i or V_d): call this plane π. There are $q(q+1)$ lines in π itself, on each of which there are q^2+q+1 planes, one of which is π again. There are, therefore, $(q+1)(q^2+q)$ planes on the point that have only a line in common with π. The difference, q^4, is the number of planes in AG(4,q) which have only the single point p in common with π. Since there are q^2 points in π, at each of which there are q^4 such planes, there are q^6 planes in AG(4,q) that have only a single point in common with V_d and hence are candidates to be the unknown key, V_i. By hypothesis, each plane counted at one of the points of π has no other point in common with π, so no plane has been counted twice.

By a similar line of argument, given a point, x, not on π, and a point, p, in π, there are q^2+q+1 planes lying on both x and p, i.e., containing the line $\langle p,x \rangle$.

There are q+1 lines in π lying on p, each of which defines a plane containing the point x. Therefore there are q^4 planes lying on the point x (i.e., consistent with one of the private pieces of information) that intersect π in only a single point, and hence candidate keys.

Finally, there is a single plane lying on any two of the independent points (meaning that they are on a line skew to π) and a point in π. Since there are q^2 points in π, there are q^2 planes on any pair of the private points which intersect π in a single point, and hence which could be a key. Just as in the previous two examples, we see that the uncertainty about the key has gone from $O(q^6)$ to $O(q^4)$ to $O(q^2)$ and finally to 0, as the concurrence has progressed from an outsider, to one insider to two insiders and, finally, to an authorized concurrence of three insiders.

What we have observed in the preceding examples can be stated precisely. Let $\dim(\mathbf{S}) = n$, $\dim(U) = k$, $\dim(V) = n-k$ and $\dim(U \cap V) = 0$; i.e., a configuration of the type depicted in Figure 5, then we have the following.

Theorem:

The dimension of the space of (n-k)-flats in $\mathbf{S}$ lying on δ independent points, $0 \leq \delta \leq n-k$ is

$$k(n-k-\delta+1) \quad .$$

Although the statement of the theorem is altered for our purposes, a proof can be found in many sources; Somnerville [A3], for example.

Prepositioned Schemes

It should be obvious by this point that one way to preposition a shared control scheme in such a way that the participants will be powerless to recover the secret until they are later enabled to do so, is to go ahead and field the private pieces of information, but to withhold the identification of the domain V_d until such time as the scheme is to be activated. That way even if all of the insiders should conspire to pool their private pieces of information in an attempt to recover the secret before the domain is revealed, the most that they can do is to reconstruct the indicator V_i and hence to learn that p is a point in the subspace V_i instead of possibly being any point in $\mathbf{S}$, which is all that an outsider knows. There is a problem, though, with this simple approach which is best illustrated using two small examples of shared secret schemes analyzed earlier.

In the example of a 2-out-of-ℓ shared secret scheme shown in Figure 1, both V_i and V_d were lines in the plane $\mathbf{S}$. Since a plane is 2-dimensional in both points and lines, i.e., it requires two shares of information (two cordinate values) to

specify either one, the same amount of information would have to be communicated to identify p as a general point in **S** as would have to be communicated to identify V_d. This might seem to indicate that two shares of information would be needed to activate the scheme, instead of the obvious minimum of a single share. Given V_i (or else V_d) p is no longer an arbitrary point in the plane but rather an unknown point on a line, whose specification requires only one share of information. Similarly, given that p is constrained to be a point on V_i, V_d no longer need be free to be an arbitrary one of the q^2 lines in the plane not parallel to the y-axis, but can instead be restricted to be one out of a set of q lines in which one line lies on each point of V_d. One easy way to do this would be to preposition an x-coordinate, x_d, different than the point at which V_i intersects the x-axis at the time the scheme is set up. Later, when the scheme is to be activated, the y intercept of the line V_d through the points x_d and p is all that would need to be communicated to permit V_d to be determined. Thereafter, any two of the participants could recover V_i using their private points, and hence recover the secret p.

If we consider the 3-out-of-ℓ scheme shown in Figure 7 in which **S** is 4-dimensional and V_d is a plane, the problem is much more difficult to deal with since 4-space is 6-dimensional in planes while the secret is only 2-dimensional in information content. While a similar, but more complex, resolution is possible in which four out of the six needed shares of information would be prepositioned along with the private pieces of information required to set up the shared secret scheme, and the remaining two shares communicated at the time the scheme is to be activated, there is a more efficient (and general) way to implement such schemes. Table 2, tabulating the dimension of the space of m-flats in an n-dimensional space, suggests how difficult this problem can become. If V_i and V_d were both three dimensional, which only permits a 4-out-of-ℓ shared control, the space of 3-flats is already 12-dimensional, meaning that twelve shares of information are required to identify V_d.

Table 2.

Dimension of the space of m-flats in an n-dimensional space.

	m							
n	0	1	2	3	4	5	6	7
1	1							
2	2	2						
3	3	4	3					
4	4	6	6	4				
5	5	8	9	8	5			
6	6	10	12	12	10	6		
7	7	12	15	16	15	12	7	
8	8	14	18	20	18	14	8	

The problem, arising in our earlier identification of V_i with a cryptographic key, is that the revelation of the secret was equated with the identification of the

point p at which the secret is determined. p is not itself the secret, but rather some entropy preserving function evaluated with p as an argument reveals the actual secret. In several examples this function was taken to be either the projection of p onto one or more of the natural coordinate axes or else the value of the variables parameterizing a surface at p. Instead, consider p to be a normal cryptographic key, say a 56-bit key for the DES, and let the information that is to be communicated to enable the system be a cipher, which when decrypted with the key will reveal the secret plaintext. Clearly, this implementation solves both of the objectives of a prepositioned shared secret scheme. If the participants cheat and misuse their private pieces of information, all that they can do is recover the shared cryptographic key. Since the cipher hasn't yet been communicated, they have no information whatsoever about the secret plaintext. On the other hand, any plaintext whatsoever can be revealed without having to change the private pieces of information, simply by communicating the cipher that will decrypt with the fixed (shared) key into the desired text.

To illustrate this implementation, consider again the simple 2-out-of-ℓ scheme shown in Figure 1 when used with the DES encryption algorithm. The plane in this case would be $AG(2,2^{56})$. Each private piece of information would consist of 112 bits, 56 of which would have to be kept secret by the participant, and 56 of which need only be protected against substitution, alteration or destruction or loss. V_d, or rather two shares of information (112 bits) adequate to determine V_d, would be prepositioned at the time the scheme was set up. Once this has been done, any two of the participants, using their private pieces of information, could determine V_i and hence recover p which in this case would be a 2-tuple in $AG(2,2^{56})$. There is no reason to not use the simplest entropy preserving function available; namely, let the secret DES key be the y coordinate of p, since by the constraints on the construction in this example all 2^{56} possible values are equally likely. Thus an authorized concurrence could recover the DES key at any time after the scheme was set up, however they could not recover the secret(s) until such time as the cipher was communicated. In those applications where it was either tolerable or acceptable that a proper concurrence be able to recover the secret at any time after the scheme was fielded, the cipher(s) could be prepositioned along with the private pieces of information. In situations such as are addressed in this paper, the cipher(s) could be withheld until it is desired that the scheme be enabled, at which time the minimum of one share of information would have to be communicated for each secret that is to be revealed.

Conclusion

The conclusion was the abstract for this paper: Secret sharing is simply a special form of key distribution.

Appendix

The purpose of this appendix is to bring together the simple geometrical results on which the construction of shared secret schemes depends and to exhibit in detail several small examples illustrating such things as duality, multilevel and multipart schemes, and which also show the way in which the key is gradually revealed as a function of the concurrence involved. We will work only in the finite affine spaces AG(n,q). Theorems will be stated without proof, since the proofs are easily found in many sources; Sommerville [A3] or Hirschfeld [A1,A2], for example.

Define a quantity

$$\varphi(n,m;q) = \begin{cases} \prod_{i=0}^{m-1} \frac{(q^n - q^i)}{(q^m - q^i)} & 1 \le m \le n \\ \text{or} & \\ 1 & m = 0 \end{cases}$$

then we have the following enumerative theorems.

Theorem 1:

The number of distinct m-flats in AG(n,q) is

$$q^{n-m}\,\varphi(n,m;q) \quad .$$

Theorem 2:

The number of distinct m-flats in AG(n,q) passing through k+1 linearly independent points, $k \ge 0$, is

$$\varphi(n-k,m-k;q) \quad .$$

Theorem 2 is normally stated in terms of the number of m-flats passing through a given k-flat, but since in shared control schemes the private pieces of information are normally points in the space, it is illuminating to state the result in terms of linearly independent sets of k+1 points, i.e., of a collusion of k+1 insiders.

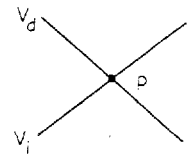
Example 1, which is the same as the example shown in Figure 1 of the text, shows the format we will use for all of the examples. The concurrences are self-explanatory. The second column will, for a single level scheme, show the number of flats of the same dimension as the indicator lying on the points exposed by the concurrence. Theorem 1 gives this value for an the outsider and Theorem 2 for all other concurrences. If V_d is unknown, then this is the equivocation faced by the collusion (concurrence) in guessing the value of the key. If V_d is known, then only those potential keys that intersect V_d in a single point are candidates to be the actual key. In Example 1 as we have already pointed out in the text, the outsider knows that the indicator must be a line, i.e., one out of the q^2+q total lines in AG(2,q), if he also knows V_d, then he need not consider any of the q lines in

Example 1.

S is 2-dimensional.

V_d is 1-dimensional

2-out-of-ℓ scheme.
(V_i is 1-dimensional).



concurrence	lines lying on the exposed points	candidate keys	possible values for the secret
outsider	$q^2 + q$	q^2	q
1 insider	$q + 1$	q	q
≥ 2 insiders	1	1	1

AG(2,q) that do not intersect V_d. In other words, only the q^2 lines that do intersect V_d in a single point are then candidates to be the key. This same format is used in all of the other examples as well. The essential point in all of the examples is that the candidate keys are (by design) uniformly distributed on the set of possible values the secret could take for all improper concurrences of the participants.

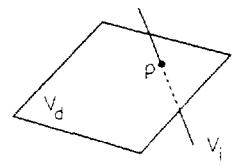
Examples 2 and 3 demonstrate the principle of duality in the smallest configuration in which it occurs. The reader should note the difference in the uncertainty as to the identity of the key from among the candidate keys in the two cases. Example 4, based on the same geometric configuration as examples 1 and 2 is again the smallest configuration in which a multilevel shared control scheme can be realized; in this case a two-level scheme in which level 1 is a 2-out-of-ℓ scheme and level 2 is a 3-out-of-ℓ scheme. The private pieces of information for the level 1 participants are points on the line V_{i_1} lying in the plane V_{i_2} and intersecting V_d in the point p, i.e., indicating p. Similarly, the private pieces of information for the

Example 2.

S is 3-dimensional

V_d is 2-dimensional

2-out-of-ℓ scheme.
(V_i is 1-dimensional).



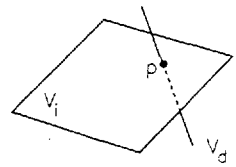
concurrence	lines lying on the exposed points	potential keys	possible values for the secret
outsider	$q^2(q^2+q+1)$	q^4	q^2
1 insider	q^2+q+1	q^2	q^2
≥ 2 insiders	1	1	1

Example 3.

S is 3-dimensional.

V_d is 1-dimensional

3-out-of-ℓ scheme.
(V_i is 2-dimensional).



concurrence	planes lying on the exposed points	candidate keys	possible values for the secret
outsider	q^3+q^2+q	q^3	q
1 insider	q^2+q+1	q^2	q
2 insiders	q+1	q	q
≥ 3 insiders	1	1	1

Example 4.

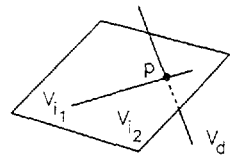
S is 3-dimensional

V_d is 1-dimensional

Two Levels:

Level One, 2-out-of-ℓ scheme.
(V_{i_1} is 1-dimensional).

Level Two, 3-out-of-ℓ scheme.
(V_{i_2} is 2-dimensional).



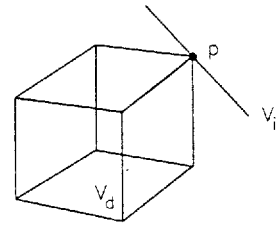
concurrence	lines lying on exposed points	planes lying on exposed points	candidate key lines lines	candidate key planes	pv for the secret
outsider	$q^2(q^2+q+1)$	$q(q^2+q+1)$	$q(q^2+q)$	q^3	q
1 level one insider	q^2+q+1	q^2+q+1	q	q(q+1)	q
1 level two insiders	q^2+q+1	q^2+q+1	q	q(q+1)	q
1 level one, and 1 level two insider		q+1		q	q
2 level two insiders		q+1		q	q
≥ 2 level one insiders	1		1		q
≥ 3 level two insiders		1		1	

Example 5.

S is 4-dimensional

V_d is 3-dimensional

2-out-of-ℓ scheme.
(V_i is 1-dimensional).



concurrence	lines lying on the exposed points	potential keys	possible values for the secret
outsider	$q^3(q^3+q^2+q+1)$	q^6	q^3
1 insider	q^3+q^2+q+1	q^3	q^3
≥ 2 insiders	1	1	1

level two participants are points in general position (no three collinear) in the plane V_{i_2}. Although it is not germane to this paper, we remark that no pair of the level 2 points can be collinear with a level 1 point, otherwise the three participants who held those points would only be capable of reconstructing a line in V_{i_2} skew to V_d, and hence they would be unable to recover the secret, contrary to the requirement that any person from level 1 in cooperation with any two from level 2 should be able to do so. In a separate paper [44], the author has solved the problem of optimally choosing the sets of private points in a two-level scheme of the type depicted in Example 4. In the table, the blank entries in the array for poten tial or candidate keys for V_{i_1} when a collusion involves two persons merely indicates that the additional parties to the concurrence in this case do not further restrict the possibilities over what a single participant did.

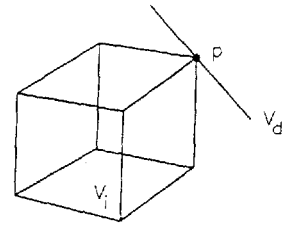
Examples 5 and 6 are included primarily because this dual configuration is the smallest that can be used to illustrate multipart shared control schemes, as shown in Example 7. Lines V_1 and V_2 in the 3-dimensional indicator V_i are skew, both with respect to each other and, of course, by construction with respect to V_d. The participants in each part would be given points on their parties' line as their private pieces of information to form two independent 2-out-of-ℓ shared control schemes. In such a control scheme it should require the concurrence of at least two persons from each part to recover the secret. The construction obviously satisfies the sufficiency of such a concurrence since the pairs of participants suffice to reconstruct the skew lines V_1 and V_2 which span the 3-flat V_i which in turn indicates the point p on V_d. Necessity however is somewhat more delicate. It is conceivable that the line defined by the point held by a member of part 1 and the point held by a member of part 2 could intersect V_d, in which case the concurrence of only two persons would know with certainty that they had recovered the secret (this presupposes that V_d is known a priori). Similarly, it is conceivable that a plane defined by one of

Example 6.

S is 4-dimensional.

V_d is 1-dimensional

4-out-of-ℓ scheme.
(V_i is 3-dimensional).



concurrence	planes lying on the exposed points	candidate keys	possible values for the secret
outsider	$q^4+q^3+q^2+q$	q^4	q
1 insider	q^3+q^2+q+1	q^3	q
2 insiders	q^2+q+1	q^2	q
3 insiders	q+1	q	q
≥ 4 insiders	1	1	1

the lines (V_1 or V_2) and a point on the other line (a concurrence of only three persons) might intersect V_d, which would have to be the point p since the plane is in the 3-flat V_i which itself has only a single point of intersection with V_d. It might appear that it would be a difficult problem to avoid all of these unacceptable configurations, that we might even be compelled to test for all possible unacceptable concurrences and eliminate from consideration for use as private pieces of information, points on the lines V_1 and V_2 that result in such configurations. In fact, we do this, but without any necessity for testing. We use a special case of a much more general result from classical geometry [A3].

Theorem:

Given a pair of skew lines in a 3-space and a point not on either of the lines, there is a unique line lying on all three.

In this restricted form, the result is easy to see; the line V_1 and the point p determine a plane in V_i, say π_1. Similarly, V_2 and p determine a plane π_2. π_1 and π_2 intersect in a line lying on p and intersecting V_1 in a point p_1 and V_2 in a point p_2. p_1 cannot be used as one of the private pieces of information for the participants in part 1, and p_2 cannot be used in part 2. With these points eliminated, clearly no collusion of two or three participants can recover the secret since the flats their points determine will all be skew to V_d.

This is a particularly interesting example since it was devised to make it possible to share control of a treaty controlled action between two national control teams in such a way that at least two participants from each control team must con-

Example 7.

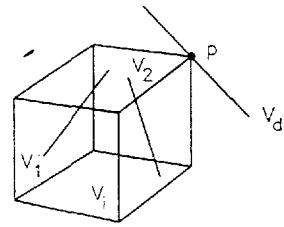
S is 4-dimensional.

V_d is 1-dimensional

Two Parts:

Part 1, 2-out-of-ℓ scheme.
(V_1 is 1-dimensional).

Part 2, 2-out-of-ℓ scheme.
(V_{2i} is 2-dimensional).



$V_1 \cap V_2 = \phi$ $\quad \dim(V_1 \cup V_2) = \dim(V_i) = 3$

concurrence	3-spaces lying on the exposed points	candidate keys	possible values for the secret
outsider	$q(q^3+q^2+q+1)$	q^4	q
1 insider from either part	q^3+q^2+q+1	q^3+q^2	q
1 insider from each part	q^2+q+1	q^2+q	q
≥ 2 insiders from either part	1	1	1

cur before the controlled action can be initiated; say between the U.S. and the U.S.S.R.

It is an easy matter to extend this example to include other parties in such a way that so long as at least two participants from at least two of the parties concur the controlled action could be initiated. For example, the UN could be a third party and the action should be possible to initiate so long as at least two out of the UN, U.S. or U.S.S.R. concur. To see how this can be achieved, let ℓ be the line lying on p, p_1 and p_2. Let V_3 be any line in V_i skew to V_1 and V_2 which intersects ℓ in a single point p_3. All of the other points on V_3 are available for use as private pieces of information for the UN team. By the same sort of argument given above, it is easy to see that no improper concurrence of participants from among the three parties can define (with their private points) a flat that intersects V_d, hence no unauthorized concurrence can recover the secret. On the other hand, any collection of participants that includes at least two members from each of two of the control teams will define a pair of skew lines in V_i, and hence, V_i, and thence p.

There are a very large number of other control schemes which can be realized using this geometrical configuration, some of which were described in Table 1. We mention only one, since it is indicative of a different type of partitioning of capability. In V_i, choose a plane V_1 skew to V_d. Points in general position in this plane can be used to realize a 3-out-of-ℓ scheme, not to recover p but to recover the plane V_1. Another participant of higher, but not absolute, authority is

Example 8.

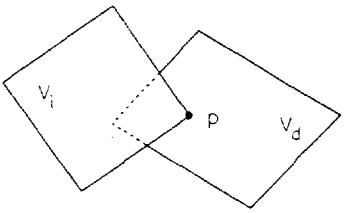
S is 4-dimensional.

V_d is 1-dimensional

Two Parts:

Part 1, 2-out-of-ℓ scheme.
(V_1 is 1-dimensional).

Part 2, 2-out-of-ℓ scheme.
(V_2 is 1-dimensional).



$V_1 \cap V_2 = \phi$ $\quad \dim(V_1 \cup V_2) = \dim(V_i) = 3$

concurrence	3-spaces lying on the exposed points	candidate keys	possible values for the secret
outsider	$q(q^3+q^2+q+1)$	q^4	q
1 insider from either part	q^3+q^2+q+1	q^3+q^2	q
1 insider from each part	q^2+q+1	q^2+q	q
$\geq$ 2 insiders from either part	1	1	1

given a point in V_i not in V_1 and not collinear with p and any point used in the plane V_1, nor coplanar with p and any pair of points used in V_1. These conditions are easily satisfied using the more general version of the theorem used to construct the usable point sets in Example 7. It now requires the concurrence of any three members of the one class and of the unique participant to initiate the controlled action. Clearly, no unauthorized concurrence, which could include the worst case of the unique participant and any two of the other class, could define a flat that intersected V_d, and hence they could not recover the secret. It should be obvious that for even such a simple configuration as shown in Example 7 that the range of possible control schemes is enormous.

Example 8 is included for a double purpose -- besides illustrating a perfect shared control scheme; it also illustrates a commonly used imperfect scheme, which we describe as a convincing argument that these abstract geometrical configurations are already "real world" solutions to problems of shared control. In the body of the paper, we mentioned the U.S. policy of the two-man control of nuclear weapons, and of the information needed to enable and hence to use these weapons. For some classes of weapons this controlling information takes the form of four symbols from an appropriate alphabet, i.e., 1-out-of-q symbols. In order to satisfy the two-man rule, this information is partitioned so that one team knows only two of the symbols, i.e., their private piece of information is a plane in a 4-space consisting of

all of the 4-tuples of symbols in which the two that they know are fixed. Similarly, the other team knows another plane in the 4-space. Since by the rank formula, any two planes in a 4-space that do not lie in a common 3-dimensional subspace intersect in a single point, the two planes intersect in a single point: the combination. This scheme is imperfect since insiders have a better chance of guessing the secret than outsiders, but it is a shared control scheme (two party) based on the geometrical configuration shown in Example 8.

Example 9.

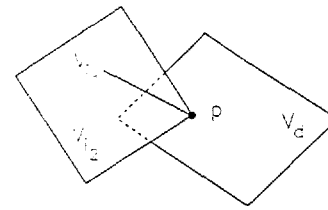
S is 4-dimensional

V_d is 2-dimensional

Two Levels:

Level One, 2-out-of-ℓ scheme
(V_{i_1} is 1-dimensional)

Level Two, 3-out-of-ℓ scheme
(V_{i_2} is 2-dimensional)



concurrence	lines lying on exposed points	planes lying on exposed points	candidate key lines	candidate key planes	pv for the secret
outsider	$q^3(q^3+q^2+q+1)$	$q^2(q^2+1)(q^2+q+1)$	$q^2(q^3+q^2)$	q^6	q^2
1 level one insider	q^3+q^2+q+1	$(q^2+1)(q^2+q+1)$	q^2	q^4	q^2
1 level two insiders	q^3+q^2+q+1	$(q^2+1)(q^2+q+1)$	q^2	q^4	q^2
1 level one and 1 level two insider		q^2+q++1		q^2	q^2
2 level two insiders		q^2+q+1		q^2	q^2
$\geq$ 2 level one insiders	1		1		1
$\geq$ 3 level two insiders		1		1	

References

A1. J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Oxford Mathematical Monographs, Oxford University Press, New York, 1985.

A2. J.W.P. Hirschfeld, Projective Geometries Over Finite Fields, Oxford Mathematical Monographs, Oxford University Press, New York, 1979.

A3. D.M.Y. Sommerville, An Introduction to the Geometry of N Dimensions, Dover Publications, Inc., New York, 1958.

Note: This bibliography includes all of the papers on shared secret or threshold schemes which the author is aware of (April 1989). Although only a few of the references appearing here are cited in this paper, it has been included for its own value to other researchers.

1. C. A. Asmuth and G. R. Blakley, "Pooling, Splitting and Reconstituting Information to Overcome Total Failure of Some Channels of Communication," Proc. IEEE Computer Soc. 1982 Symp. on Security and Privacy, Oakland, CA, Apr. 26-28, 1982, pp. 156-169.

2. C. Asmuth and J. Bloom, "A Modular Approach to Key Safeguarding," IEEE Trans. Info. Theory, Vol. IT-29, No. 2, Mar. 1983, pp. 208-210.

3. J. Benaloh and J. Leichter, "Generalized Secret Sharing and Monotone Functions," Crypto'88, Santa Barbara, CA, Aug. 21-25, 1988, Advances in Cryptology, to appear.

4. J. C. Benaloh, "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret," Crypto'86, Santa Barbara, CA, Aug. 11-15, 1986, Advances in Cryptology, Vol. 263, Ed. by A. M. Odlyzko, Springer-Verlag, Berlin, 1986, pp. 251-260.

5. L. Berardi, M. DeFonso and F. Eugeni, "Thereshold Schemes Based on Criss-Cross Block Designs," Private Communication.

6. L. Berardi and F. Eugeni, "Geometric Structures, Cryptography and Security Systems Requiring a Quorum," Proc. 1987 ATTI del Primo Simposio Nazionale su Stato e Prospettive della Ricerca Crittografica in Italia, Rome, Italy, Oct. 30-31, 1987, pp. 127-133.

7. A. Beutelspacher and K. Vedder, "Geometric Structures as Threshold Schemes," Proc. 1987 IMA Conference on Cryptography and Coding Theory, Cirencester, England, Oxford University Press, to appear.

8. A. Beutelspacher, "Enciphered Geometry: Some Applications of Geometry to Cryptography," Proceedings of Combinatorics'86, Annals of Discrete Mathematics, 37, North-Holland, 1988, pp. 59-68.

9. A. Beutelspacher, "How to say 'No'," Eurocrypt'89, Apr. 11-13, 1989, Houthalen, Belgium, Advances in Cryptology, Springer-Verlag, Berlin, to appear.

10. G. R. Blakley and R. D. Dixon, "Smallest Possible Message Expansion in Threshold Schemes," Crypto'86, Santa Barbara, CA, Aug. 11-15, 1988, Advances in Cryptology, Vol. 263, Ed. by A. M. Odlyzko, Springer-Verlag, Berlin, 1986, pp. 266-274.

11. G. R. Blakley and C. Meadows, "Security of Ramp Schemes," Crypto'84, Santa Barbara, CA, Aug. 19-22, 1984, Advances in Cryptology, Vol. 196, Ed. by G. R. Blakley and D. Chaum, Springer-Verlag, Berlin, 1985, pp. 411-431.

12. G. R. Blakley and L. Swanson, "Security Proofs for Information Protection Systems," Proc. IEEE Computer Soc. 1981 Symp. on Security and Privacy, Oakland, CA, Apr. 27-29, 1981, pp. 75-88.

13. G. R. Blakley, "One-time Pads are Key Safeguarding Schemes, Not Cryptosystems: Fast Key Safeguarding Schemes (Threshold Schemes) Exist," Proc. IEEE Computer Soc. 1980 Symp. on Security and Privacy, Oakland, CA, Apr. 14-16, 1980, pp. 108-113.

14. G. R. Blakley, "Safeguarding Cryptographic Keys," Proc. AFIPS 1979 Nat. Computer Conf., Vol. 48, New York, NY, June 1979, pp. 313-317.

15. J. R. Bloom, "A Note on Superfast Threshold Schemes," preprint, Texas A&M Univ., Dept. of Mathematics, 1981.

16. J. R. Bloom, "Threshold Schemes and Error Correcting Codes," Am. Math. Soc., Vol. 2, 1981, pp. 230.

17. J. Box, D. Chaum and G. Purdy, "A Voting Scheme," Crypto'88, Santa Barbara, CA, Aug. 21-25, 1988, Advances in Cryptology, to appear.

18. E. F. Brickell and D. R. Stinson, "The Detection of Cheaters in Threshold Schemes," 18th Annual Conference on Numerical Mathematics and Computing, Sept. 29-Oct. 1, 1988, Winnipeg, Manitoba, Canada, Congressus Numerantium, Vol. 68-69, to appear 1989.

19. E. G. Brickell, "Some Ideal Secret Sharing Schemes," 3rd Carbondale Combinatorics Conference, Oct. 31, 1988, Carbondale, IL, J. Combinatorial Mathematics and Combinatorial Computing, to appear.

20. D. Chaum, Claude Crepeau and I. Damgard, "Multiparty Unconditionally Secure Protocols," 4th SIAM Conference on Discrete Mathematics, San Francisco, CA, June 13-16, 1988, abstract appearing in SIAM Final Program Abstracts: Minisymposia, #M-28/3:20pm, pp. A8.

21. D. Chaum, "How to Keep a Secret Alive: Extensible Partial Key, Key Safeguarding, and Threshold Systems," Crypto'84, Santa Barbara, CA, Aug. 19-22, 1984, Advances in Cryptology, Vol. 196, Ed. by G. R. Blakley and D. Chaum, Springer-Verlag, Berlin, 1984, pp. 481-485.

22. D. Chaum, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups," Memo. No. UCB/ERL/M79/10, Univ. of Calif, Berkeley, ERL 1979; also, Ph.D. dissertation in Computer Science, Univ. of Calif., Berkeley, 1982.

23. 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, Oct. 1985, pp. 383-395.

24. G. I. Davida, R. A. DeMillo and R. J. Lipton, "Protecting Shared Cryptographic Keys," Proc. IEEE Computer Soc. 1980 Symp. on Security and Privacy, Oakland, CA, Apr. 14-16, 1980, pp. 100-102.

25. M. De Soete and K. Vedder, "Some New Classes of Geometric Threshold Schemes," Eurocrypt'88, May 25-27, 1988, Davos, Switzerland, Advances in Cryptology, Vol. 330, Ed. by C. G. Günther, Springer-Verlag, Berlin, pp. 57-76.

26. A. Ecker, "Tactical Configurations and Threshold Schemes," preprint (available from author).

27. Paul Feldman, "A Practical Scheme for Non-iteractive Verifiable Secret Sharing," Proc. 28th Annual Symp. on Foundations of Comp. Sci., Los Angeles, CA, Oct. 12-14, 1987, IEEE Computing Soc. Press, Washington, D.C., 1987, pp. 427-437.

28. S. Harari, "Secret Sharing Systems," Secure Digital Communications, Ed. by G. Longo, Springer-Verlag, Wien, 1983, pp. 105-110.

29. 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).

30. M. Ito, A. Saito and T. Nishizeki, "Multiple Assignment Scheme for Sharing Secret," preprint (available from T. Nishizeki).

31. E. D. Karnin, J. W. Greene and M. E. Hellman, "On Secret Sharing Systems," IEEE International Symposium on Information Theory, Session B3 (Cryptography), Santa Monica, CA, Feb. 9-12, 1981, IEEE Trans. Info. Theory, Vol. IT-29, No. 1, Jan. 1983, pp. 35-41.

32. S. C. Kothari, "Generalized Linear Threshold Scheme," Crypto'84, Santa Barbara, CA, Aug. 19-22, 1984, Advances in Cryptology, Vol. 196, Ed. by G. R. Blakley and D. Chaum, Springer-Verlag, Berlin, 1985, pp. 231-241.

33. K. Koyama, "Cryptographic Key Sharing Methods for Multi-groups and Security Analysis," Trans. IECE Japan, Vol. E66, No. 1, 1983, pp. 13-20.

34. C. Matsui, K. Tokowa, M. Kasahara and T. Namekawa, "Notes on (K,N) Threshold Scheme," Proc. Joho Riron To Sondo Ooyo Kenkyukai, VII-th Symposium, Kinugawa, Japan, Nov. 5-7, 1984, pp. 158-163 (in Japanese); The VII-th Symposium on Information Theory and Its Applications, English translation available from G. J. Simmons.

35. R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes," Com. ACM, Vol. 24, No. 9, Sept. 1981, pp. 583-584.

36. C. Meadows, "Some Threshold Schemes Without Central Key Distributors," Crypto'88, Santa Barbara, CA, Aug. 21-25, 1988, Advances in Cryptology, to appear.

37. M. Merritt, "Key Reconstruction," Crypto'82, Santa Barbara, CA, Aug. 23-25, 1982, Advances in Cryptology, Ed. by D. Chaum, R. L. Rivest and A. T. Sherman, Plenum Press, New York, 1983, pp. 321-322.

38. M. Mignotte, "How to Share a Secret," Workshop on Cryptography, Burg Feuerstein, Germany, Mar. 29-Apr. 2, 1982, Cryptography, Vol. 149, Ed. by T. Beth, Springer-Verlag, Berlin, 1983, pp. 371-375.

39. R. von Randow, "The Bank Safe Problem," Discrete Applied Mathematics, 4, 1982, pp. 335-337.

40. P. J. Schellenberg and D. R. Stinson, "Threshold Schemes from Combinatorial Designs," submitted to the Journal of Combinatorial Mathematics and Combinatorial Computing.

41. A. Shamir, "How to Share a Secret," Massachusetts Inst. of Tech. Tech. Rpt. MIT/LCS/TM-134, May 1979. (See also Comm. ACM, Vol. 22, No. 11, Nov. 1979, pp. 612-613.)

42. G. J. Simmons, "How to (Really) Share a Secret," Crypto'88, Santa Barbara, CA, Aug. 21-25, 1988, Advances in Cryptology, to appear.

43. 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. 68-69, to appear 1989.

44. G. J. Simmons, "Sharply Focused Sets of Lines on a Conic in PG(2,q)," 20th Southeastern International Confeence on Combinatorics, Graph Theory & Computing, Feb. 20-24, 1989, Boca Raton, FL, Congressus Numerantium, to appear 1989.

45. D. R. Stinson and S. A. Vanstone, "A Combinatorial Approach to Threshold Schemes," Crypto'87, Santa Barbara, CA, Aug. 16-20, 1987, Advances in Cryptology, Ed. By Carl Pomerance, Springer-Verlag, Berlin, 1988, pp. 330-339.

46. D. R. Stinson and S. A. Vanstone, "A Combinatorial Approach to Threshold Schemes," SIAM J. Disc. Math, Vol. 1, No. 2, May 1988, pp. 230-236. (This is an expanded version of the paper appearing in Advances in Cryptology: Proceedings of Crypto'87, Vol. 293, Ed. By Carl Pomerance, Springer-Verlag, Berlin, 1988.)

47. 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.

48. H. Unterwalcher, "A Department Threshold Scheme Based on Algebraic Equations," Contributions to General Algebra, 6, Dedicated to the memory of Wilfried Nöbauer, Verlag B. G. Teubner, Stuttgart (GFR), to appear Dec. 1988.

49. H. Unterwalcher, "Threshold Schemes Based on Systems of Equations," Österr. Akad. d. Wiss, Math.-Natur. Kl, Sitzungsber. II, Vol. 197, 1988, to appear.

50. H. Yamamoto, "On Secret Sharing Schemes Using (k,L,n) Threshold Scheme," Trans. IECE Japan, Vol. J68-A, No. 9, 1985, pp. 945-952, (in Japanese); also published as "Secret Sharing System Using (k,L,n) Threshold Scheme," Electronics and Communications in Japan, Part 1, Vol. 69, No. 9, 1986, pp. 46-54.

51. H. Yamamoto, "On Secret Sharing Communication Systems with Two or Three Channels," IEEE Trans. Info. Theory, Vol. IT-32, No. 3, May 1986.

52. H. Yamamoto, "Coding Theorem for Secret Sharing Communication Systems with Two Noisy Channels," IEEE Trans. Info. Theory, to appear.

53. T. Uehara, T. Nishizeki, E. Okamoto and K. Nakamura, "Secret Sharing Systems with Matroidal Schemes," Trans. IECE Japan, Vol. J69-A, No. 9, 1986, pp. 1124-1132, (in Japanese; English translation available from G. J. Simmons) presented at the 1st China-USA International Conference on Graph Theory and its Applications, Jinan, China, June 1986. English summary by Takao Nishizeki available as Tech. Rept. TRECIS8601, Dept. of Elect. Communs., Tohoku University, 1986.