HOW TO (REALLY) SHARE A SECRET[1]

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

Introduction

In information based systems, the integrity of the information (from unauthorized scrutiny or disclosure, manipulation or alteration, forgery, false dating, etc.) is commonly provided for by requiring operation(s) on the information that one or more of the participants, who know some private piece(s) of information not known to all of the other participants, can carry out but which (probably) can't be carried out by anyone who doesn't know the private information. Encryption/decryption in a single key cryptoalgorithm is a paradigm of such an operation, with the key being the private (secret) piece of information. Although it is implicit, it is almost never stated explicitly that in a single-key cryptographic communications link, the transmitter and the receiver must unconditionally trust each other since either can do anything that the other can.

Even if it can't be assumed that all of the elements in a system are trustworthy, so long as there exists at least one identified unconditionally trustworthy element (individual or device), it is generally possible to devise protocols to transfer trust from this element to other elements of unknown trustworthiness to make it possible for users to trust the integrity of the information in the system even though they may not trust all of the elements. A paradigm for such a protocol is the cryptographic key distribution system described in ANSI X9.17 which makes it possible for

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

S. Goldwasser (Ed.): Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 390-448, 1990.

users who have had no previous contact, nor any reason to trust each other, to trust a common cryptographic session key because they each unconditionally trust the key distribution centers (KDC).

The more common (and hence the more realistic) situation is that there are no identified unconditionally trustworthy elements in a system. Instead, the most that can be assumed is that while any specific element may be suspect, i.e., possibly subject to either deliberate or inadvertent compromise, and hence untrustworthy insofar as the faithful execution of the part of the protocol entrusted to it, that there are some (unidentified) elements in the system which are trustworthy. Under these circumstances there is apparently only one way to improve the confidence one can have in the integrity of the system over the confidence one has in the integrity of the individual elements, and that is by introducing some form of redundancy. To protect against random failures of devices, this is commonly achieved by parallel or by series-parallel operation of redundant elements or by even more complex logical interconnections. In the case of individuals, though, since the failure may be both deliberate and clandestine, redundancy typically takes the form of requiring the concurrence of two or more knowledgeable persons to carry out an action. A paradigm for this would be the well-known two-man control rule for access to, or the control of, nuclear weapons. The k-out-of-ℓ shared secret or threshold schemes first discussed by Blakley [10] and Shamir [33], and subsequently by numerous other authors [see the bibliography], are a natural generalization of this concept. In fact, shared secret schemes exist that are adequate to the task of insuring shared capability if all that is needed is a simple k-out-of-ℓ participation for the reconstruction of a secret piece of information essential to the system functioning. Ideally, any collusion of k-1 or fewer of the holders of information -- even if they pool their private pieces of information in an effort to cheat

the system -- should have no better chance of success than an outsider who knows no private information at all. Schemes in which this latter condition holds have been characterized as "perfect" by Stinson [33,34]. We merely remark that several perfect k-out-of-ℓ shared secret or threshold schemes have been described in the literature. Many of these schemes are also unconditionally secure in the sense that the security they provide is independent of the computing time or power that an opponent may bring to bear on subverting the system, or, put in another way, even with infinite computing power would-be cheaters can do no better than guess (with a uniform probability distribution on the choices available to them) at the secret. If the secret is a function (such as one of the coordinates, or the largest coordinate, or the norm of the coordinates, etc.) of a (secret) point in some n-dimensional vector space over a finite field GF(q), then by choosing q large enough we can make the system be as secure as we wish for an arbitrary $k < \ell$. These are "plain vanilla" shared secret schemes for which several implementations have been devised [see the references flagged with an * in the bibliography]. Consequently, there is no difficulty in providing (and implementing) simple shared secret schemes for arbitrary choices of k and ℓ and for any desired level of security.

Real-world applications, however, require rather considerably more in the way of capabilities in shared secret schemes than a simple k-out-of-ℓ concurrence for an action to be initiated. In this paper we will do two things: first enumerate and briefly describe eight of these extended capabilities and then (in compliance with the unanimous recommendation of the reviewers) describe in detail how to realize only one class of these extensions in order to keep the length of this paper within reasonable bounds.

Capabilities Required for Various "Real" Applications of Shared Secret Schemes

The new capabilities (over and above the simple k-out-of-ℓ shared secret schemes) are:

- Compartmented[2] k_i-out-of-ℓ_i shared secret schemes in which the private information is partitioned in such a way that reconstruction of the secret requires a specified level of concurrence by the participants in some specified number (perhaps all) of the compartments (k_i concurrence is required of the members of the i^{th} compartment).
- Multilevel[2] k_i-out-of-ℓ_i shared secret schemes in which the private information is partitioned into two or more levels (classes) in such a way that concurrence of the specified number of participants at any one of the levels will permit the secret to be reconstructed (k_i concurrence by the members of the i^{th} or higher levels is required).
- Extrinsic as opposed to intrinsic shared secret schemes, i.e., schemes in which the value of a private piece of information to the reconstruction of the secret depends only on its functional relationship to other pieces of private information, and not on its information content (in an information theoretic sense).
- Prepositioned shared secret schemes in which the holders of the private pieces of information are unable to recover the secret information, even if they all collude to do so, until such time as the scheme is activated by communicating additional information.
- Prepositioned shared secret schemes in which the same collection of private pieces of information can be

2. We have adopted standard security terminology in which information is classified into levels (classifications) and into compartments (need to know) to describe the two types of partitioning of the private pieces of information in a shared secret scheme.

used to reveal different secrets depending on the choice of the activating information.

- Proof of correctness of the reconstructed secret information to a confidence of $\approx 1-P_d$, where P_d is the probability of guessing the secret.
- Tolerance of erroneous inputs of some number, s, of the private pieces of information, i.e., the correct secret information will be calculated even though s of the inputs are in error, where s is a design parameter.
- A cryptographically secure mnemonic technique to make it possible for the participants to recover a private piece of information that they can't remember using a piece that they can.

It is easy to conceive of situations in which it might be desirable that some action require a preselected level of concurrence by two or more parties in order for the action to be executed. For example, a treaty might require that two out of a Russian control team and two out of a U. S. team agree that the controlled action is to be taken before it could be initiated. What is different about such a compartmented scheme from the simple k-out-of-ℓ schemes, is that no matter how many of the participants of one nationality (compartment or part) concur, the action is to be inhibited unless the preselected number of the other nationality also concur. Clearly, there is nothing special about partitioning the private information into only two parts (compartments). The specific application will determine how many parts are needed to effect the type of concurrence desired.

In *Animal Farm*, George Orwell's animals have a slogan "All animals are equal, but some animals are more equal than others" which is certainly descriptive of the apportionment of authority in most organizations. While it is not true, for example, that two members of the Joint Chiefs of Staff

equal one President, it is easy to conceive of circumstances in which the President might wish to delegate authority to the Joint Chiefs to initiate some action with the proviso that "If two of you agree that the circumstances warrant, then this is what you should do...." On the other hand, there are also plausible scenarios in which the concurrence of larger numbers of persons with lesser authority (and responsibility) could act in the stead of smaller numbers of higher authority. For example, it might well be the case that any senior officer of a bank can authorize an electronic funds transfer up to some specified limit, but that in the absence of a senior officer, any two senior tellers could do so, etc. The point is that authority in the real world is typically different for different classes (levels) -- like it or not -- and that consequently control schemes for information, i.e., shared secret schemes, need to reflect this class structure. We describe such schemes as multilevel k_i-out-of-ℓ_i schemes, where realistically the number of levels is small and the values of the k_i are determined by the requirements of the application. The notion of a hierarchy of shared secret schemes was already anticipated in Shamir's paper, but in a form (intrinsic) that as we shall see has very serious deficiencies for real-world applications.

In a multilevel system, the persons holding the private pieces of information are grouped into classes (levels) such that the private information one class has is more (or less) valuable in recovering the secret than that which another class has. In all of the perfect shared secret schemes that we know of, the private pieces of information are not used to directly reconstruct the "secret" itself but instead are used to reconstruct an algebraic variety (a line, a plane or other linear subspace in many of the previously reported schemes but more generally complex varieties defined by polynomial constraints in an n-dimensional space) whose description, i.e., precise specification, is unknown to the

holders of the private information. If there were no other constraints, a multilevel system would be trivial to realize for any set of k_i, since a simple shared secret scheme is possible for each k_i. To realize a multilevel system, the i^{th} class could simply have its own separate and distinct k_i-out-of-ℓ_i shared secret scheme. This might be acceptable in some applications, but not in general. If, for example, a bank vault can be opened by either two VP's or three senior tellers, it would probably be unacceptable that one VP and two senior tellers not be able to open it. If the capabilities (private pieces of information) of members of the more privileged classes are to be usable when they cooperate with members of other less privileged classes, then the schemes are forced to be functionally related. We know how to do this in two ways, which leads into the discussion in the next paragraph of extrinsic and intrinsic shared secret schemes.

To illustrate an intrinsic shared secret scheme, assume that we have a 4-out-of-ℓ scheme in some n-dimensional space over GF(q). The private pieces of information are points in the space, i.e., n-tuples over GF(q), chosen so that any set of four of these points suffice to define the secret but any set of three or fewer will provide no information whatsoever about the secret. Clearly we could construct a 2-out-of-ℓ class by making the private pieces of information for the members of this more privileged class consist of pairs of the points out of the original set, i.e., two n-tuples. In fact, this is how Shamir proposed to realize what he called hierarchical control schemes. This type of construction of the private pieces of information is what we call an intrinsic scheme in which the value of a piece of private information (i.e., its contribution toward recovering the secret information) is internal to the private information itself. In an information theoretic sense, the more privileged pieces of information are more valuable simply because they contain more information about the shared secret. This

means that the most privileged members would be responsible for the largest amounts of private information, and in the case of several levels with widely differing k_i perhaps responsible for infeasibly much information for them to handle (securely). Such hierarchical schemes have been discussed before, not only by Shamir [32], but by Ito, et al. [23], and other authors.

In an extrinsic scheme all the private pieces of information are alike in an information theoretic sense, say the coordinates of a single point in some n-dimensional space, and its value in recovering the secret is determined not by anything internal to that piece of information but rather by the functional relation between that particular piece of private information (point) and the private pieces of information (points) held by the other participants. In other words, the value is determined by something external to the private pieces of information. An extrinsic scheme does not penalize the more privileged classes by requiring them to handle more information than members of less privileged classes.

Prior to the results described here, there was no means known to realize either extrinsic multilevel control schemes or compartmented (multipart) schemes. Ito, Saito and Nishizeki [23] had devised an intrinsic general access control scheme which, however, can not be extended to an extrinsic scheme and all (k,ℓ) threshold schemes can be adapted in an obvious way to intrinsic (hierarchical) multilevel schemes similar to those Shamir proposed [32].

In a prepositioned shared secret scheme, say a simple k-out-of-ℓ scheme, the ℓ pieces of private information can all be placed in the hands of the participants in advance of when the scheme will be needed; with the added property that until the scheme is activated by providing some additional information, that even if all ℓ of the private pieces of information were to be exposed in violation of the protocol, the secret would not only not be exposed but it would be

just as unlikely to be recovered, i.e., just as secure, as if none of the private pieces of information had been compromised. Only when the additional piece of information is made available does the system become activated, after which any set of k of the pieces of private information will allow the secret to be recovered. It is worth remarking that there is a trivial realization of a prepositioned shared secret scheme by simply making $\ell = k-1$, i.e., by designing a k-out-of-ℓ shared secret scheme, in which all of the private pieces of information when taken together are inadequate to recover the secret, but such that one more piece (the activating information) is required. We are not interested in such schemes since they fail to meet the most fundamental requirement of k-out-of-n systems, namely, avoiding the necessity to have to bring together a designated set of k private pieces of information in order to reconstruct the secret information. The main reason for being interested in prepositioned shared secret schemes is that the (relatively) large quantity of private information can be disseminated, authenticated, etc., in times of low stress and easily available communication and the small quantity of information needed to activate the scheme can be communicated under extreme duress -- such as a state of advanced alert for the military or even the outbreak of war.

A relatively new discovery is the possibility of setting up a prepositioned shared secret scheme, i.e., prepositioning the private pieces of information, with the additional property that there are several activating pieces of information available, each of which would lead to the recovery of a distinct secret piece of information. This could be a very valuable characteristic in some military applications where there are several different actions -- any one of which higher command might wish to enable -- but subject to a k-out-of-ℓ shared secret control in execution. The basic idea is that one needn't change the private pieces of information (which would require a great deal of communication,

authentication, etc., and presents an enormous human factors problem) in order to change the secret protected by the shared secret scheme.

If the consequence of exercising a shared secret scheme is immediate -- for example, if after the VP's enter their private pieces of information, the bank vault door either opens or it doesn't -- then there is no need to provide a supplemental indication that the correct value for the secret has been recovered. If however the effect is distant, in either time or physical location, then it may be vital to the acceptability of the scheme that the participants have an immediate indication that the correct value of the secret has been reconstructed. If, for example, a shared secret scheme is to be used to control the enabling of a warhead in a missile, it is clearly desirable to have a confirmation that the correct value has been entered prior to launch as opposed to learning that the weapon had not been enabled after its arrival at the target. Providing an indication that the correct secret has been reconstructed is similar to the function of error detecting codes which, in probability, indicate when a received code word is in error, although we hasten to add that the functions are not identical. This last remark requires more discussion than is appropriate to an abbreviated description of the extended capabilities for shared secret schemes, but basically it is possible to cause a shared secret scheme to indicate when it has reconstructed the correct secret even though the secret itself was unknown prior to the reconstruction (and not available from any other source for direct comparison after reconstruction to determine its validity). This is similar to being able to verify a digital signature without being able to utter one. In general (but not in all cases which is the basis of the preceding remark), this costs one more piece of private information to achieve than is necessary for a simple shared secret scheme, i.e., k+1 instead of k inputs of private pieces of information.

If the capability discussed in the preceding paragraph was only similar in function to error detecting codes, the capability of recovering from erroneous inputs of private pieces of information is precisely the same as the function of error correcting codes. In other words, we can design shared secret schemes so that up to s of the inputs can be in error and not only will the correct value for the secret be found, but if we desire, a proof of correctness can be output to show that the right value has been reconstructed. Clearly this cannot be done for free, since if only k inputs are needed and s can be in error, k-s of the participants could collude and input their correct private pieces of information, after which any s random inputs would suffice to recover the secret. Roughly speaking (not so roughly as a matter of fact since the result is true within one required input) k+s+1 inputs of private pieces of information are needed to guarantee k-concurrence (i.e., k-man control), recovery from s erroneous entries, and a positive indication of the correctness of the secret value recovered.

Several authors have addressed the problem of detecting cheating (falsified inputs) in a secret sharing or threshold scheme [13,16,17,28,36]. McEliece and Sarrwate [28] actually construct a secret sharing scheme based on a Reed-Solomon error detecting and correcting code which can tolerate s incorrect entries. In their construction any set of k + 2s participants (holders of private pieces of information) will be able to correctly reconstruct the secret so long as at most e of the inputs are incorrect or falsified. Tompa and Woll [36] give a construction for an unconditionally perfect k-out-of-ℓ shared secret scheme. In both of these constructions the participants will (probably) be able to tell that cheating has occurred, but they cannot necessarily determine who the cheaters are. The combinatorial scheme of Brickell and Stinson [13] is also an unconditionally perfect k-out-of-ℓ scheme which also has the property

that the cheater(s) will be identified in the process (with high probability).

Finally, in this list of capabilities, if k-1 inputs of correct private pieces of information are to provide no information whatsoever about the secret information, then every other piece of private information must appear completely random even though k-1 pieces are known. This says that an unknown n-tuple, if the setting is in an n-dimensional space over some GF(q), must itself appear random, not in all n coordinates, but effectively in α of them if the secret is α dimensional; by which we mean that the equivocation about the secret must be the same as the uncertainty of guessing a point in an α-dimensional space over GF(q). q must be large enough to provide the desired level of security against random picking of points. By present-day computational standards, 56 bits is regarded as barely large enough to be secure, witness the continuing debate over the long-term security of the DES, but 100 bits is unquestionably secure against a brute-force search of the key space. However even the modestly secure limit of 100 bits is a 20 alphanumeric character string that must appear totally random by the remarks above, which is beyond anyone but a stage memory expert's ability to recall. Since shared secret schemes are not communication channels, the standards for the security of a communications cryptographic key do not necessarily apply. But even at 56 bits or 12 alphanumeric characters as required for a DES key, it is still impossible for most people to recall a random string of this length as their private piece of information. Fortunately, there exists an approved mnemonic technique for generating a one-time key of sufficient length, using easily remembered private phrases or verses, to permit the secure recovery of something that can't be remembered (the random appearing private piece of information) from something that can (the private phrase).

There are a great many other technical aspects of shared secret schemes which need to be considered, however the main ones which we have been able to identify that affect the operational acceptability of these schemes have been described here.

The Basic Construction for Shared Secret Schemes

We illustrate the essential elements in the construction of shared secret schemes using the simplest possible example: a 2-out-of-ℓ scheme. Let the secret be a single numerical value, i.e., having a 1-dimensional uncertainty, which is equivalent to the identification of a point, p, on a line, L_d.

Figure 1.

If we now consider L_d to be embedded in the projective plane PG(2,q), and randomly choose any other line, L_i, in the plane, $L_i \neq L_d$, then the private pieces of information can be taken to be distinct points on L_i, none of which are the point p. L_i is kept secret, only the fact that such a line exists, etc., is public knowledge. For the purposes of this paper, L_d will be assumed to be known a priori. There are applications in which this is not the case, but we will not have time to discuss them here.

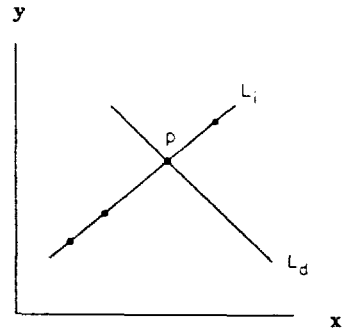


Figure 2.

Any pair of points on L_i determine the line and thence its intersection with L_d; the point p. On the other hand, knowing any one of the points, q, on L_i leaves p totally undetermined since for each choice of a point, r, on L_d there exists a unique line <q,r> lying on q and r which could (with equal probability) be the unknown line L_i -- in which case the (secret) point of intersection of L_i with L_d would be the arbitrary point r. Therefore every point on L_d is an equally likely candidate to be the secret point p given either no knowledge of the private pieces of information (points on L_i) or else of only one private piece. In this example, since p could (equally likely) be any point on the line, $P_d = 1/q+1$, while the number of participants, ℓ, can be as great as q, i.e., any point on L_i other than p could be used as a private piece of information.

It should be remarked that the point p, although it is unknown in advance of the 2-out-of-ℓ scheme being exercised, is not itself the secret. The secret is recovered by evaluating a predesignated function, f, at the point p: f could be as simple as one of the coordinate values of p or the distance of p from some reference point or it could be a much more complex function. Whatever the function is, it is assumed to be known a priori so that as soon as p is determined, so is the secret. There are restrictions on f that must be satisfied in order for it to be suitable for this sort of application. For example, if f were a simple parity check (on the coordinate values) mapping the points on L_d into the set (0,1), then the uncertainty about the secret would be at most one bit irrespective of how many different values p could take. For our purposes, we assume that f conserves entropy, i.e., that the uncertainty about f(p) is the same as the uncertainty about p.

Returning to the simple example shown in Figure 2; p was an (unknown) point in a larger set -- all of the points on the line L_d. The secret revealing function, f, is defined (at least) on all of the points in V_d and as mentioned

above, conserves entropy. It is worth noting that it is immaterial (to the secret sharing scheme) whether f is also defined for points in the plane not on L_d. In our construction of shared secret schemes, the line L_d will be replaced by a more general type of geometrical object -- an algebraic variety, V_d, in some n-dimensional space: i.e., the set of points in L_d satisfying a set of specified polynomial constraints. This collection of points, any one of which could be the unknown point p, we will refer to as the domain (variety) for the function f hence the notation V_d. The line L_i can be thought of as "pointing" to the point p in L_d. In the most general formulation, the private pieces of information (points in the n-dimensional space) suffice to define a second algebraic variety, V_i, whose function it is to "point" to the point p in V_d. We will say that V_i is the indicator (variety) using the term indicator with its preferred meaning of pointing to or indicating a specific item, i.e., of pointing to the point p. p we will call the index. Without saying precisely how the private pieces of information determine the indicator, pictorially our shared secret schemes are of the form:

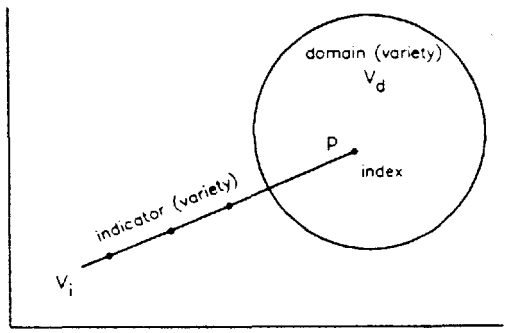


Figure 3.

where V_i and V_d are two algebraic varieties having only the single point p in common. The indicator V_i is shown as a line in Figure 3 to emphasize the fact that it is pointing to a unique point in V_d, but in general it can be any

algebraic variety satisfying the conditions for a shared secret scheme. In order for the scheme to be acceptable, we will also require that any compromise (collusion) of less than the required number and types of private pieces of information will leave every point in V_d an equally likely candidate to be the unknown point p. As mentioned earlier Stinson has characterized shared secret schemes meeting this latter condition as perfect [33,34] and we will adopt that terminology also.

An example of a perfect 3-out-of-ℓ scheme is shown in Figure 4.

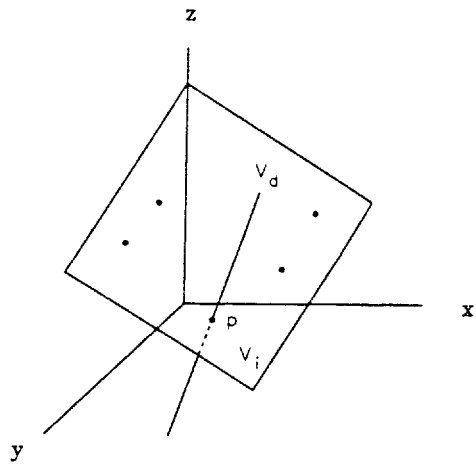


Figure 4.

The private pieces of information are points in general position in the indicator (plane) V_i, i.e., none of them are p and no three (including p) are collinear. The domain is the set of points on the line V_d. f could be any entropy conserving function defined on the points in V_d, say the value of the z-coordinate if V_d is chosen not to lie in a plane perpendicular to the z axis. To see that this scheme is perfect, consider the case in which two holders of private pieces of information collude in an attempt to cheat the system. The two points that they know defines a line, ℓ, in V_i which does not intersect V_d. Given any point r on V_d there exists a unique plane $<\ell,r>$ lying on ℓ and r which

is equally likely to be the unknown variety V_i as that determined by any other point on V_d. Consequently, for this collusion all points on V_d are equally likely candidates to be the unknown point p, and the scheme is perfect. It is worth remarking about the construction of Figure 4 that while the secret can be any one of q+1 points on the line, V_d, so that the security of the scheme is $P_d = 1/q+1)$, the number of participants, ℓ, could be as great as q or q+1 depending on whether q is odd or even, respectively. This follows from the well known result that the maximum number of points that can be selected in the plane PG(2,q) such that no three of them are collinear is a set of q+1 points on a conic (plus the nucleus of the conic of q is even) and that the point p is neither collinear with any pair of the private points nor equal to any one of them. The point of the remark is that while we wish to make P_d be small, i.e., for the scheme to be secure, which requires that q be very large, ℓ is normally quite small. There is a price exacted for this unused capacity as we shall see later.

The construction of perfect shared secret schemes proceeds in two steps. First we must find two families of algebraic varieties which intersect pairwise in single points, i.e., one of which can be considered to indicate a point in the other. In order for such a construction to be applicable to constructing shared secret schemes it must also be the case that all of the points in the domain variety can be indicated by the varieties of the other type, and in fact, the even stronger restriction must hold that each point in the domain is an equally likely index of the indicator (variety) as the indicator ranges over all possible values. The second step is: given two families of algebraic varieties satisfying these conditions, one must devise ways to define a unique member of one of these families that requires the specified level of concurrence on the part of the holders of the pieces of private information. In the two simple examples this took the form of 2-out-of-ℓ or

3-out-of-ℓ concurrence in order for the indicator (a line or a plane in the examples) to be reconstructed. In general, the required concurrence can be arbitrarily complex; for example, at least one member of each of n committees must be present for a vote to be binding or two, or three, etc. The point is that we want it to be possible to reconstruct the indicator variety only when the specified concurrence occurs and for it not only to be impossible in all other cases, but that the even stronger result will hold that every point in the domain, V_d, will be equally likely to be p in all other cases (collusions).

Our constructions will generally be based on a simple result from point geometry -- the rank formula:

$$r(S) + r(T) = r(S \cap T) + r(S \cup T) \tag{1}$$

which holds for all subspaces S and T of the n-dimensional projective space PG(n,q) or Q^n in short. For notational consistency the empty subspace is defined to have rank 0 and dimension -1. To illustrate how (1) applies, consider the following construction: π_1 and π_2 are planes in a 4-dimensional space, Q^4, which do not lie in a common 3-dimensional subspace. $\pi_1 \cup \pi_2 = Q^4$ in this case, and we have

$$\begin{aligned} r(\pi_1) + r(\pi_2) &= 3 + 3 = r(\pi_1 \cup \pi_2) + r(\pi_1 \cap \pi_2) \\ &= 5 + r(\pi_1 \cap \pi_2) \quad . \end{aligned}$$

Therefore,

$$r(\pi_1 \cap \pi_2) = 1$$

and

$$\pi_1 \cap \pi_2 = p \quad , \quad p \text{ a point.}$$

Restated; in 4-dimensional space any pair of planes that do not lie in a common 3-dimensional subspace intersect in a point. Clearly this is a candidate construction for the pair of varieties we need to construct a shared secret

scheme. We still have to show that the desired uniformity of intersection holds, i.e., that for a fixed π_1, as π_2 ranges over all of the planes in Q^4 that do not intersect π_1 in a line, each point of π_1 will occur equally often as the intersection $\pi_1 \cap \pi_2$. To see that this is true, fix π_1 and choose any line ℓ in Q^4 skew with respect to π_1. Let q be an arbitrary point in π_1, then $\langle q,\ell \rangle = \pi$ is the unique plane lying on q and ℓ. If $\pi \cap \pi_1$ were a line ℓ^*, i.e., if $\pi \cup \pi_1$ is a 3-dimensional subspace of Q^4, then ℓ^* and ℓ are both in π and hence must intersect in a point. But this point would be in both ℓ and π_1 which contradicts the assumption that ℓ is skew to π_1. Therefore π and π_1 intersect in only the single point q. But q was an arbitrary point in π_1, hence for each skew (to π_1) line ℓ there is a unique plane on ℓ intersecting π_1 at point q. Now let ℓ range over all lines skew to π_1, etc.

We now show how the geometrical result of the preceding paragraph can be used to construct a 3-out-of-ℓ shared secret scheme to conceal a 2-dimensional secret. V_d is an arbitrary, but known a priori, plane in the 4-dimensional projective space Q^4. V_i is a randomly chosen plane which does not lie in any common 3-dimensional space with V_d. A possible selection procedure for V_i is to choose a point q, $q \notin V_d$, and a point r, $r \notin \langle V_d \cup q \rangle$. Note that $q \notin V_d$ implies by the rank formula that $\langle V_d \cup q \rangle$ is 3-dimensional. $\langle q,r \rangle$ is a line skew to V_d. Now choose (with a uniform probability distribution) a point $p \in V_d$ and define

$$V_i = \langle p, \langle q,r \rangle \rangle \quad .$$

The private pieces of information will be points in V_i none of which are p, and no three of which (including p) are collinear. Clearly this is a 3-out-of-ℓ shared secret scheme which can indicate any point p in V_d. A simple adaptation of the uniformity argument proves that the scheme is perfect even if two of the pieces of private information

(points in V_i) are combined in an attempt to cheat the system. In this case the secret can be any one of the q^2+q+1 points in the plane V_d, so that $P_d = 1/(q^2+q+1)$, while ℓ is at most q or q+1 depending on whether q is odd or even as remarked earlier.

There are a couple of other important points to make about shared secret schemes in general. In the construction of a perfect 3-out-of-ℓ shared secret scheme to secure a 1-dimensional secret shown in Figure 4, the private pieces of information were points in a 3-dimensional space, i.e., 3-dimensional themselves. An alternative construction for a perfect 3-out-of-ℓ scheme which also secures a 1-dimensional secret is:

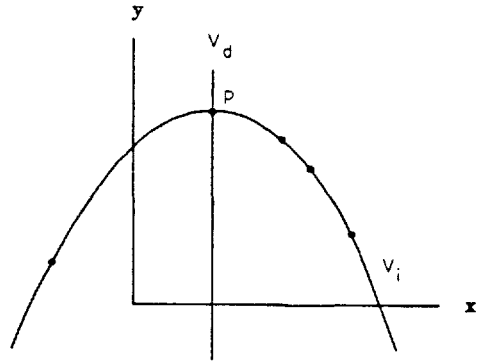


Figure 5.

where any three points on V_i suffice to define the quadratic curve and hence the point p at which it intersects V_d. The private pieces of information in this case are 2-dimensional, i.e, points in the plane. These two examples show that not only is a shared secret scheme not fixed by the specification of the level of concurrence (k-out-of-ℓ) and the dimension of the secret which is to be secured, but that even the dimension of the space in which the scheme is implemented -- and hence the dimension of the private pieces of information -- is not determined.

This leads to the second, and most important, observation: the information in the private pieces of information is not all of the same type in the sense of how it must be secured. To see this, consider the simple 2-out-of-ℓ scheme shown in Figure 2. The private pieces of information are points on the line L_i, i.e., 2-tuples of the form (x_j,y_j). It is not necessary to keep both of these coordinate values secret in order to protect the secret from improper recovery. One of the coordinate values can be kept secret, say y_j, which we indicate by $\textcircled{y_j}$, while the other need not be kept secret but only its integrity (against substitution, alteration, deletion, etc.) needs to be insured. It is easy to show that in the most damaging collusion possible for this scheme (an insider misusing his private information $(x_j, \textcircled{y_j})$ and the exposed values $x_1,\ldots,x_\ell$ for all of the other participants) that all points on V_d will be equally likely candidates to be the index p and hence that the scheme is still perfect.

Clearly the information content in a private piece of information must be at least or great as in the secret, otherwise a collusion of (k-1)-parties would be faced with a lesser uncertainty in guessing a missing piece of private information (and hence in recovering the secret) than the uncertainty they are assumed to have about the secret -- clearly a contradiction. In the example just given, $H(y_j) = H(p)$, i.e., the information content in the part of the private piece of information that has to be kept secret is exactly the same as the uncertainty about the secret itself. As we shall see for the constructions described here this is always possible. What does differ from one realization of a shared secret scheme to another (having the same specifications) is the amount of information in the private pieces of information which doesn't have to be kept secret.

Perfection: At What Price?

The reader has probably wondered why we introduced two varieties in our model for shared secret schemes, one of which was defined by the private pieces of information, and then defined the index to be their intersection instead of simply defining the index directly in terms of the private pieces of information; and whether both of the varieties are necessary. A discussion of the main reason for introducing the domain variety (in addition to the clearly essential indicator variety) will be deferred until a later paper however the simple answer to the question is that the domain can be dispensed with -- but only by sacrificing perfection for the shared secret schemes when $k < \ell$.

To illustrate the difficulty, consider the simplest possible example of a k-out-of-ℓ shared secret schemes, $k < \ell$, in which the private pieces of information directly determine the index shown in the construction in Figure 6. The index in this example is a point, p, in the plane and the private pieces of information are a pencil of lines on p.

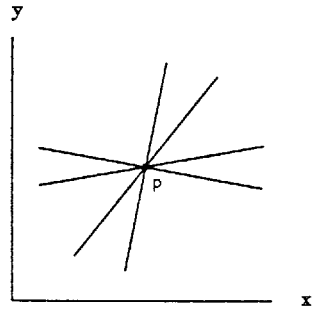


Figure 6.

Since any two of the lines determine p, while a knowledge of any one of them leaves p (linearly) indeterminate this is a 2-out-of-ℓ S^3 for a 1- (2?)-dimensional secret. The ambiguity as to the dimension of the secret is due to the fact that each insider knows that p must lie in the 1-dimensional variety which he knows and hence p is only 1-dimensional in

uncertainty to him, while to an outsider p has 2-dimensional uncertainty since it could be any point in the plane.

Since k = 2 in this example, the only improper insider collusion possible is that of a lone individual trying to misuse his private piece of information. As a result, this example does not adequately illustrate what happens when k > 2 and the index is derived directly from the private pieces of information without the aid of an indicator. To show what happens in general, let the secret, p, be a point in a 3-dimensional space and the private pieces of information be a bundle of planes all containing p, but no three of which contain any common line. This is clearly a 3-out-of-ℓ shared secret scheme for a 3-dimensional (to outsiders) secret: any pair of the planes defines a line containing p which, since it isn't in any of the other planes, must intersect each of them at p.

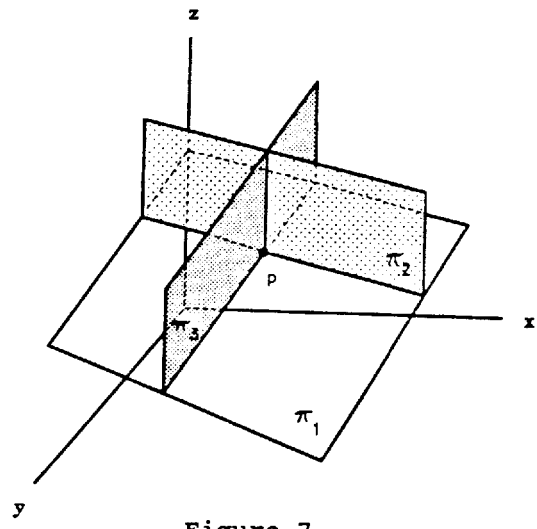


Figure 7.

However, the secret is only of 2-dimensional uncertainty to any single insider since he knows p must be in the plane which is his private piece of information and of only 1-dimensional uncertainty to any pair of insiders since they know p must be common to both their planes and must there-

fore be contained in the line of intersection of the two planes. The problem is that the index is contained in each of the private varieties in all of these examples (and in general in this type of shared secret schemes) and is identified by the intersection of sufficiently many of the private varieties to determine the index. As a result, the successive intersections define a sequence of, if not monotonically decreasing, at least nonincreasing (in dimension) varieties converging to the point p. It isn't possible to make this sequence of intersections be equal to the dimension (≥ 1) of the secret through the penultimate, (k-1)-st, step in the reconstruction of the secret and then on the final step at which the k-th private variety is introduced to suddenly become of dimension 0. This might be possible if the order in which the various pieces of private information had to be used could be specified in advance, but a shared secret scheme must be immune to compromise by all subsets of k-1 or fewer insiders and in whatever order they choose to collude. Hence this isn't possible. Consequently, erosion of the uncertainty about the index with increasing numbers of persons in a collusion is an inherent shortcoming of all shared secret schemes in which the index (set) is determined directly from the private pieces of information.

An interesting observation, though, is that this need not be true if $k = \ell$. For example, a perfect 2-out-of-2 shared secret scheme is easy to realize (for a secret of any dimension). One of the participants is given a random point, r, in V_d and the other the vector sum (Vernam encryption) of p with r, say p-r. Clearly this is a perfect 2-out-of-2 scheme irrespective of the dimension of V_d. Pictorially, if V_d is 1-dimensional, we have

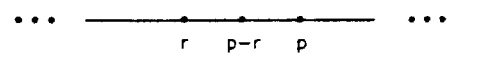


Figure 8.

Both the secret and the private pieces of information are 1-dimensional. Their sum recovers the 1-dimensional secret, p. To extend this scheme to a perfect k-out-of-k 1-dimensional shared secret scheme, $k > 2$, it is only necessary to give k-1 of the insiders random numbers, r_i, as their private pieces of information and the Vernam cipher $p - \Sigma r_i$ to the k-th individual. In spite of the apparent asymmetry in this assignment procedure which appears to give more significant information to the holder of $p - \Sigma r_i$ than to the individuals whose private information is one of the r_i, this is not the case and any collusion of k-1 or fewer holders of private pieces of information will be totally uncertain of p in the sense that it could (equally likely) be any point in V_d. Obviously, by construction the sum of all k of the points is p. Consequently, not only are all of the pieces of private information equivalent (in uncertainty) but more importantly there is no erosion of the uncertainty about p until the k-th and final piece of information becomes available, at which point p is determined.

This construction for 1-dimensional k-out-of-k shared secret schemes in which there is no indicator but in which there is also no erosion of the uncertainty about the index, p, with the compromise of fewer than k of the private pieces of information can easily be extended to the concealment of secrets of any dimensionality. Let p be an m-dimensional secret (point in Q^n). Choose the k private pieces of information to be k-1 randomly chosen points, r_i, in V_d, and the point $p - \sum_{i=1}^{k-1} r_i$. The combining operation will be the vector sum -- component addition in the underlying finite field. Under these circumstances any subset of k-1 or fewer of the points will leave the index completely undetermined since it could be any point in V_d while the vector sum of all k will, by construction, be p. We remarked earlier that it wasn't possible to make the dimension of the secret and of the private pieces of information both be n in a perfect k-out-of-ℓ

shared secret schemes in the space Q^n if $k < \ell$. What we have seen in the constructions of this section is that there are perfect shared secret schemes in which an indicator doesn't appear and in which this common dimensionality is possible if $k = \ell$. We will utilize these perfect k-out-of-k shared secret schemes, later in a class of constructions for realizing compartmented shared secret schemes in which more than a single group of persons must concur in order for a controlled action to occur.

The emphasis on dimension in the preceding discussion is slightly misleading. While it is certainly true that for a fixed ground space Q, less information is needed to specify a point in Q^m than in Q^n, where $m < n$, as we have already pointed out, this information is not all equally costly to generate, distribute or to protect. In fact the expensive secret part of the private information can be made to be the same in all realizations for a particular set of specifications.

The application normally dictates the level of concurrence, k, required to provide the desired level of confidence in the proper execution of the controlled action and the number of participants, i.e., the number of private pieces of information that the scheme needs to accommodate. The application also dictates the maximum probability, P_d, that can be tolerated of someone (either outsiders or an improper collusion of insiders) guessing the shared secret on whose concealment the control scheme is predicated. If the values that the secret can assume are equiprobable, then the number of such values, i.e., the number of points in the domain, $|V_d|$, must be at least

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

There may also be other parameters involved. For example, as we have pointed out earlier, it may be natural to consider the secret information as having a dimension, d, etc.

In summary, both the indicator and domain varieties are essential to the realization of a perfect shared secret scheme. Given the basic construction (concept) of having one variety point to a point in the other at which the secret is defined, the geometrical nature of the resulting shared secret schemes is virtually forced. The problem is to devise ways to insure that the desired level(s) of concurrence will define the indicator and such that no lesser level of collusion will reveal anything about it. There are also important questions connected with making such schemes be practical such as minimizing the amount of secret information that needs to be protected by the holders of the private pieces of information, or of making such schemes robust against either deliberate or unintentional erroneous inputs. However, the basic principal for constructing shared secret schemes is the same in all cases.

An Application (and Two Realizations) of Compartmented Shared Secret Schemes

We consider first the simplest possible compartmented scheme: there are two parties (compartments) to the shared control, both of whom must concur for the controlled action to be initiated. Because of the sensitivity of the action, each party wishes to impose the requirement that at least two members of their control team must agree that the action should be initiated before their party's concurrence can be obtained. To be less abstract, assume that there is some treaty controlled action that requires U. S. and U.S.S.R. concurrence for its initiation. Each country has a team of its own representatives (controllers) at the site. Because the controllers are trusted -- but not unconditionally trusted -- to carry out their nation's commitment to the protocol, each country requires that at least two of their controllers must concur before their national input to the shared control scheme is to be possible. Clearly, this is

quite a different control situation than occurs in a simple (k,ℓ) threshold scheme. In the present case, even if all ℓ of the Americans (ℓ could be a large number) and one of the Russians agree, the controlled action is to be inhibited! For simplicity, we will assume that the secret has 1-dimensional uncertainty, i.e., that it is equivalent to identifying a point on a line.

There are two approaches (using the construction for shared secret schemes described here) to constructing compartmented schemes. We will describe both of them and analyze their relative efficiencies in order to justify our choice of a preferred scheme. The first approach is to let the private information for each part(y) determine a subvariety V_j: ordinarily a (k_j-1)-dimensional subspace where the j-th part requires a k_j-out-of-ℓ_j control. These subvarieties are all chosen to be linearly independent subspaces of a common space, i.e., so that no pair of them have a point in common. The indicator variety is then the union of the required number of these subvarieties (both of them in the present example). V_d, as usual is a variety (subspace) any point of which could with equiprobability be p. We have in this case

$$V_i = V_1 \cup V_2$$

and

$$V_i \cap V_d = p \quad ,$$

where

$$\dim(V_i) = \dim(V_1) + \dim(V_2) + 1 \quad .$$

This is conceptually the simpler approach since the resulting compartmented scheme is essentially the same as we have already given for simple k-out-of-ℓ shared secret scheme. Because of the complexity of the general case, we will describe a construction of this type (for the simple two-part example) before describing the other type of construction for compartmented schemes.

We note that a 2-out-of-ℓ, $\ell > 2$, control scheme always determines a line in some space. If the line (shared variety) determined by the U. S. control team is to be independent of the line determined by the U.S.S.R. team, i.e., if the two lines are to be skew so that they do not intersect, then the subspace they span, the indicator V_i, will be 3-dimensional. The domain (variety), which is 1-dimensional from the problem statement, must be independent of the subspace spanned by the two shared varieties, hence the lowest dimensional space in which a scheme of the type we are considering could possibly be constructed would be 4-dimensional. This can be done as follows. Take as the two shared varieties a pair of skew lines, L_1 and L_2, in Q^4. The domain is a third line, V_d, skew to both L_1 and L_2. As usual in a 2-out-of-ℓ shared secret scheme, the private pieces of information will be points on the lines L_1 or L_2, subject to the side condition that none of them are on the unique line, ω, that intersects all three of the lines.[3] The points at which ω intersects the lines L_1, L_2 and V_d are q, r and p, respectively. The lines L_1 and L_2 span a 3-flat $V_i = \langle L_1, L_2 \rangle$ which does not contain V_d. Hence

$$V_i \cap V_d = p$$

which is the index for this particular shared secret scheme.

Since a clear understanding of how this scheme functions is essential to understanding the extensions to be described later, we rephrase in nonmathematical terms what has just been said geometrically. Any two members of the first group

3. Note: We prove rather more than is needed for the present construction. In Q^3 there is a unique line passing through a given point, p, and intersecting each of two skew lines L_1 and L_2, neither of which lies on p. To see this, note that p and L_1 determine a plane, π. L_2 intersects π in a point, q; $q \neq p$ by construction since L_2 does not lie on p. The line $\omega = \langle p,q \rangle$ is in π as is the line L_1, so they intersect in a point r. Hence ω is the unique line lying on p and intersecting L_1 and L_2 (in points q and r, respectively). Now consider any space Q^n, $n \geq 4$. Let L_1 and L_2 be a pair of skew lines in Q^n. L_1 and L_2 span a 3-dimensional subspace S of Q^n. Given an arbitrary (n-3)-dimensional subspace, T, of Q^n, independent of S, T intersects S in a single point, p, by the rank theorem. Let this point, p, be the point in the above construction, etc. We therefore have proven that in Q^n, $n \geq 4$, there is a unique line incident with each of a pair of skew lines and with an (n-3)-dimensional subspace independent of each of these lines.

can determine the line L_1 from their private pieces of information. Similarly any two members of the second group can determine the line L_2. Once L_1 and L_2 are known, it is easy to calculate the 3-flat they determine, in other words to determine the polynomial constraints that must be satisfied by all of the points in V_i. The domain V_d, which is assumed to be known a priori, is itself defined by a polynomial constraint. The index, p, is the unique point satisfying all of these constraints. The geometry of the construction quarantees that there is one and only one point satisfying both. Pictorially:

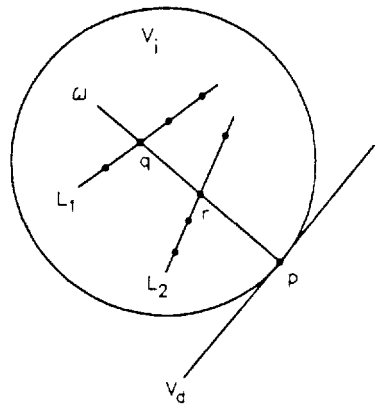


Figure 9.

The most threatening form of collusion for this scheme would be if two (or more) persons from one group and one from the other pooled their private pieces of information in an effort to defeat the control scheme. With no loss of generality, assume that L_1 has been compromised and one point, x, on L_2; $x \neq r$ by construction. To prove that the scheme is perfect we must show that every point on V_d is equally likely to be the secret datum under these circumstances. We extend Kerchoff's criteria from cryptography to shared secret schemes and assume that the geometrical nature of the scheme is known a priori to both insiders and outsiders, i.e., to all would-be cheaters. By this assumption

a participant in a collusion knows that L_1, L_2 and V_d are skew lines in Q^4 and that the secret datum is the point of intersection of $V_i = \langle L_1, L_2 \rangle$ with the line V_d.

Choose any point, u, on V_d. An opponent knows that if u is to be the secret datum, it must be collinear with a point of L_1 (which has been exposed by the collusion) and a point on the line L_2. He doesn't know L_2 of course, only that it is a line lying on x and skew to both L_1 and V_d. Let w be an arbitrary point on L_1; not one of the exposed private points (pieces of information) since by construction none of these points are the (unknown) point of intersection, q, of ω with L_1. The line $\omega^* = \langle u,w \rangle$ lies in $\langle L_1, V_d \rangle$ since $u \in V_d$ and $w \in L_1$. x is not in $\langle L_1, V_d \rangle$, however, since $L_2 \cap \langle L_1, V_d \rangle = r$ and $x \neq r$. Therefore, for each point, z, on ω^*, $z \neq u$ or w, a line $L_2' = \langle x,z \rangle$ is determined which is independent of $\langle L_1, V_d \rangle$ and for which

$$L_2' \cap \langle L_1, V_d \rangle = z \quad .$$

Consequently, if $L_2 = L_2'$, i.e., if the constructed line, L_2', were the unknown L_2, then the secret datum would be u. This is true for every choice of a point $w \in L_1$, where w is not one of the points exposed in the collusion, and for all points z on ω^*, $z \neq u$ or w. Therefore the cardinality of the set of schemes lying on L_1 and x in L_2 is the same for all choices of $u \in V_d$; which for small numbers of colluders from group one is of the order of the cardinality of a 2-flat in Q^4.

Since the private points on L_1 were chosen to be different from q, a natural question to ask is whether the equivocation about p might be a function of the number of insiders from group one who join in the collusion. To see that this is not the case consider the most extreme case possible in which ℓ equals the number of points on the line less only the excluded point, q, and all ℓ of the private points are exposed in the collusion. By elimination in this case, q is

unambiguously identified and exposed, and the only possible choice for w is w = q. For each choice of a point u ε V_d the number of schemes on L_1, x and u is the number of points on a line less two, since z $\neq$ u or q. Therefore, even in this most extreme case of collusion, all points u on V_d are equally likely to be p insofar as the colluders can determine.

Any other collusion (the line L_1 (or L_2) or else a point on each line, x ε L_1 and y ε L_2 or else a point on only one of the lines x ε L_1 (or y ε L_2)) is less damaging than the case just analyzed, i.e., the probability of the collusion improperly determining the index p cannot be increased as a result of the opponent having less information about the scheme. Therefore this construction provides a perfect two-part scheme in which each part is a 2-out-of-ℓ scheme.

To summarize, a construction of the first type to realize a perfect two-party shared secret scheme to secure a 1-dimensional secret, in which each part is a 2-out-of-ℓ control scheme, is possible in four dimensions. Although we haven't described in detail how the private information is to be partitioned into the one part (dimension) which must be kept secret and another (three dimensions) which need not be, an obvious extension to the earlier discussion of the partitioning of the private information applies here as well.

The other approach to realizing a compartmented shared secret scheme is to let the subvarieties determined by the private pieces of information individually indicate points in a space containing V_d which can be treated as inputs to the overall concurrence scheme: in the present case 2-out-of-2 since both of the parties must concur. As we have already seen, k-out-of-k schemes are special so it should come as no surprise that the compartmented scheme is also special in this case (in the sense that it doesn't represent the general behavior of such schemes). Figure 10

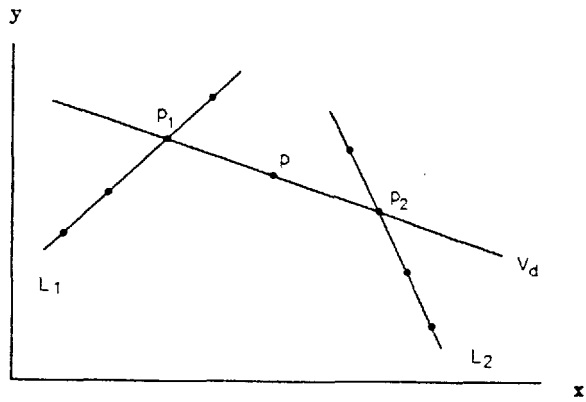
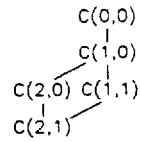


Figure 10.

shows a two-part scheme of the second type. L_1 is the subvariety (line) defined by the private pieces of information belonging to one party and L_2 is the other. The intersection of L_1 with V_d is a point p_1 which is treated as an input to the perfect 2-out-of-2 scheme defined on V_d. p_2 is determined similarly by L_2. Clearly this is a two-part scheme.

To prove that the scheme in Figure 10 is perfect, we introduce a method of proof which, while we have used it before, hasn't been explicitly stated. Given any shared secret scheme, simple, compartmented, multilevel, etc., it suffices to prove that the uncertainty about the index is the same for a more compromising collusion as it is for an outsider attack to simultaneously prove that it is the same for all lower levels of collusion dominated by the case under consideration. For simple k-out-of-ℓ schemes collusions are linearly ordered, so that it is only necessary to consider the most damaging collusion in order to prove perfection (a remark we made earlier). Compartmented and multilevel schemes however have a lattice (often partial) ordering on the collusions. For example the ordering on the five collusions C(0,0)-C(2,1)[4] is

4. The notation C(i,j) indicates a collusion in which i points from one private part and j from the other have been exposed. In a two-part scheme in which both parts require the same level of concurrence C(i,j) = C(j,i). C(0,0) is an outsider attack, etc. The notation generalizes to arbitrarily many parts in an obvious manner.



so that if the uncertainty about the index is the same for C(2,1) as it is for C(0,0), the scheme is perfect.

Now consider the scheme in Figure 10. p is only known a priori to be a point on V_d, i.e., of 1-dimensional uncertainty to collusion C(0,0). Similarly, if one of the input points, say p_1, is known and any other point on the indicator variety, say x, on L_2 is exposed -- $x \neq p_2$ by construction -- then, since for any point on V_d there is a unique line lying on it and x that could be the unknown (to the participants in the collusion) line L_2, every point on L_d is is an equally likely candidate to be p. p is therefore of 1-dimensional uncertainty to collusion C(2,1) and by the remark, to all of the other collusions as well. Hence, the shared secret scheme in Figure 10 is perfect.

The contrast between the two types of compartmented shared secret schemes is significant for the application we have been discussing and dramatic for other choices of parameters: in the present case the private information is 2-dimensional for the second type of scheme rather than 4-dimensional as was the case for the first type; and with no real difference in capability. The only difference is that in the first type, all of the points on the subvarieties which did not lie on the transversal ω were available for use as private pieces of information while in the second type, the points p_1 and p_2 had to be excluded. In both cases the part of the private information that has to be kept secret is only 1-dimensional. If there is no cost involved in insuring the integrity of the information that doesn't need to be kept secret the schemes are equally attractive, while if there is a cost the second type is the

clear winner since it involves only half as much information in the private parts.

Unfortunately, because of the difference between k-out-of-k and k-out-of-ℓ schemes the construction for the second type of compartmented system for this example fails to illustrate a very important property of this class of schemes.

The smallest example which shows what happens in general is a scheme in which there are three parts, at least two of which must concur for the controlled action to be initiated. Each part, considered separately, is a 2-out-of-ℓ control scheme. The essential feature of this example over the one discussed earlier is that the highest level concurrence is a k-out-of-ℓ, $k < \ell$ scheme instead of a k-out-of-k scheme. It is trivial to extend the construction shown in Figure 9 to this case, or to any number of parts, $k \leq q$ where the construction is in PG(4,q) for this example. To do this we simply choose (appropriately) another line, L_3, in the 3-dimensional subspace V_i to be the variety determined by the third party. By "appropriately" we mean that the three lines L_1, L_2 and L_3 must be skew by pairs so that any two of them span (determine) V_i and that they all intersect a common line ω in V_i lying on the point p. The points of intersection of ω with L_1, L_2 and L_3 -- q, r and s, respectively -- are not used as one of the private pieces of information, although any of the q other points on a line can be. This later requirement is imposed so that the proof of perfection given earlier will still hold for this case as well. Figure 11 shows the resulting construction.

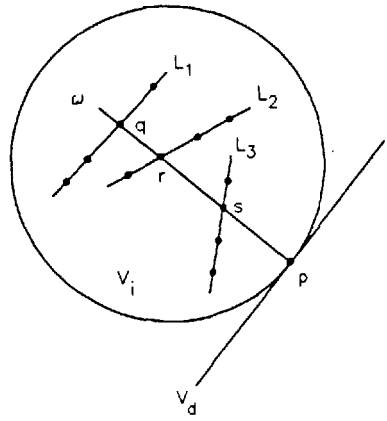


Figure 11.

We introduce the notation $\underset{c}{\cup} L_j$ or $\underset{c}{\cup} V_j$ to indicate the union of a designated concurrence of the individual parts: any two in this particular example.

$$\underset{c}{\cup} L_j = L_1 \cup L_2 = L_1 \cup L_3 = L_2 \cup L_3 = \cup L_j = V_i \quad .$$

The dimension of the space $\mathcal{S}$ in which the shared secret scheme is implemented is

$$\dim \mathcal{S} = \dim(V_d \cup V_i) = 4 \quad ,$$

and

$$V_i \cap V_d = p = (\underset{c}{\cup} L_j) \cap V_d$$

as was true in the construction given in Figure 9. Consequently, for the first type of construction, there is no significant effect in having gone from requiring a unanimous concurrence by the two parties to requiring only 2-out-of-ℓ, $\ell > 2$, concurrence. The second type of construction however is quite different from that shown in Figure 10 as is evident in Figure 12 where a 2-out-of-3 scheme is depicted.

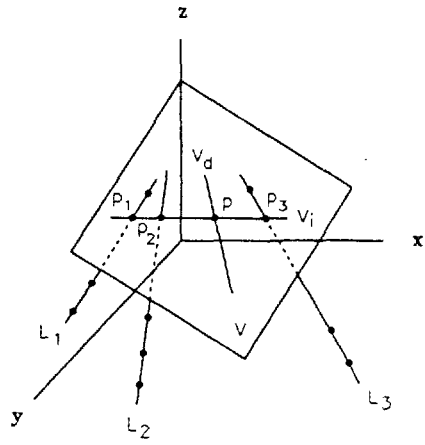


Figure 12.

A simple 2-out-of-3 scheme is implemented in the plane $V = V_i \cup V_d$. The index p is defined by the intersection of the lines V_i and V_d. What is different is that the points p_1, p_2 and p_3, any pair of which suffice to determine the indicator V_i, are themselves determined by the intersection of the lines L_1, L_2 and L_3, respectively, with the plane V, where the lines themselves are determined by any pair of the private points on them. The dimension of the containing space **8** in this construction has increased from 2 (for the 2-out-of-2 concurrence example) to 3. The fact that the dimension of the shared secret scheme of the first type remained fixed at 4 while the dimension of a scheme of the second type increased from 2 to 3 raises the question of whether there might be examples in which each type of scheme is the more efficient. We next show that this can never be the case.

In general, the first type of construction defines the indicator, V_i, by

$$V_i = \underset{c}{\cup} V_j$$

where the V_j are the varieties determined by the individual parts, irrespective of whether $k = \ell$ or $k < \ell$. In either case, the index is defined by

$$V_i \cap V_d = p = (\underset{c}{\cup} V_j) \cap V_d \quad . \tag{1}$$

In general, to realize a scheme of the second type requiring a k-out-of-ℓ concurrence by the parts, we first define a space V,

$$V = V_i \cup V_d \quad ,$$

and embed a simple k-out-of-ℓ shared secret scheme in it. V_i is an indicator (variety or subspace) in V which intersects V_d in the index p, etc., and in which any k points in V_i suffice to determine it. V itself is then considered to be in a space $\mathcal{S}$ of a dimension adequate to allow each of the subvarieties, V_j, defined by the individual parts to intersect V in only a single point, p_j. Any k of these points of intersection will suffice to determine the indicator V_i and hence the point of intersection, p, of V_i and V_d to recover the secret.

The essential point to this construction is that

$$V_i = \underset{c}{\cup} p_i = \underset{c}{\cup}(V_j \cap V)$$

and

$$V_i \cap V_d = p = (\underset{c}{\cup}(V_j \cap V)) \cap V_d \quad . \tag{2}$$

To simplify the comparison we first consider the case in which all of the parts require the same level of concurrence: k′-out-of-ℓ'. If the concurrence required of the individual parts is k-out-of-ℓ and the secret is d-dimensional, then the dimension of the containing space $\mathcal{S}$ is

$$\dim(\mathcal{S}) = kk' + d - 1 \tag{3}$$

for a scheme of the first type irrespective of whether $k = \ell$ or $k < \ell$. For a scheme of the second type,

$$\dim(S) = k' + d - 1 \tag{4}$$

if $k = \ell$, and

$$\dim(S) = k' + k + d - 2 \tag{5}$$

if $k < \ell$. For the example just analyzed, $k = k' = 2$ and $d = 1$ so that the dimension of the spaces were 4, 2 and 3, respectively. Since it must always be the case that $k \geq 2$ and $k' \geq 2$, it is easy to see that it is always possible to construct a shared secret scheme of the second type in a lower dimension space than is possible for a scheme of the first type. This is also true if the individual parts do not all require the same level of concurrence:

$$k'_1 \geq k'_2 \geq \ldots \geq k'_\ell \quad .$$

We then have, in analogy to the results above,

$$\dim(S) = \sum_{j=1}^{k} k'_j + d - 1 \tag{3*}$$

for a scheme of the first type irrespective of whether $k = \ell$ or $k < \ell$. For a scheme of the second type

$$\dim(S) = k'_1 + d - 1 \tag{4*}$$

if $k = \ell$, and

$$\dim(S) = k'_1 + k + d - 2 \tag{5*}$$

if $k < \ell$.

In summary, in spite of the simplicity of the first type of construction for compartmented shared secret schemes, it is never as efficient (in the usage of information) as schemes of the second type.

A Discussion of Exceptional Cases

It is almost as difficult to provide for unanimity in shared secret schemes as it is to secure it in real-life situations. In this section we will discuss several examples in which one or more of the parts requires unanimity of input and in which the overall control scheme may require either k-out-of-ℓ, $k < \ell$, or k-out-of-k concurrence.

The smallest -- not necessarily the simplest -- example is obtained by modifying the first problem we discussed: a two-part scheme in which each part required a 2-out-of-ℓ concurrence. If the concurrence required for one of the parts is changed from a 2-out-of-ℓ scheme to a 2-out-of-2 scheme, it isn't obvious how to construct a compartmented scheme of the first type. Recall that in this type of construction the indicator, V_i, is a subspace spanned by the varieties determined by the individual parts. In this case, since there are two parts -- both of whom must concur in order for the secret to be recovered -- V_i would be the union of the line, say L_2, determined by the 2-out-of-ℓ scheme and presumably the point, p_1, determined by the 2-out-of-2 scheme. V_i must then be a plane

$$V_i = \langle L_2, p_1 \rangle$$

The private pieces of information for the second part are points on the line L_2, etc. The problem is: where are the two points (private pieces of information) q_1 and r_1 that define p_1 for the 2-out-of-2 scheme. They can't be confined to the plane V_i, otherwise V_i would be determined by L_2 and only one of the points q_1 or r_1. Hence if the system is to

be perfect, it must be the case that the two points, q_1, and r_1, lie in a 3-space which contains V_i. Pictorially:

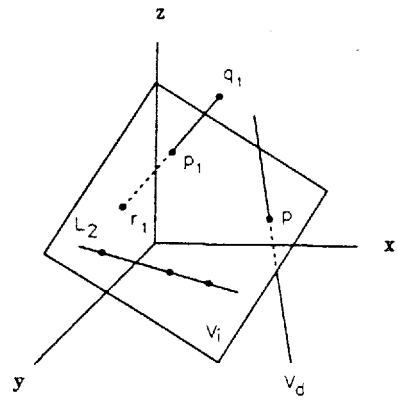


Figure 13.

p_1 cannot be a point on L_2 nor collinear with p and any point on L_2 used as one of the private pieces of information for the second part. The first condition is to insure that when the concurrence conditions are satisfied that V_i and hence p will be determined. The second is to insure that a collusion consisting of p_1 and one point on L_2 will not reveal the secret.

The construction in Figure 13 illustrates one (of the many) problems associated with k-out-of-k schemes. In this case the dimensionality of the containing space **S** suddenly ceases to obey the counting formula given earlier. If part one were a 3-out-of-3 or a 4-out-of-4 or in general a k_1-out-of-k_1, $k_1 \leq q$, concurrence scheme and part two remained a 2-out-of-ℓ scheme, **S** would still only need to be 3-dimensional; exactly as shown in Figure 13. In other words, we seem to have lost the functional dependence between the minimum dimension for the containing space **S** and the concurrence level k_1 which we had identified earlier.

Now consider a compartmented scheme of the second type for the same example. Recall that in this type of scheme,

the individual parts determine indicators that point to points in an intermediate subspace V in which the overall shared secret scheme is embedded. Since this highest level scheme is a 2-out-of-2 concurrence for this example, V need only be a line as shown in Figure 8. L_2 must be a line which intersects $V = V_d$ in a single point p_2. p_1 of course is also a point on V_d; for which $p = p_1 + p_2$. The question is: where must the points q_1 and r_1 be located? There is no reason for them to be outside of the plane determined by L_2 and V_d, $\pi = \langle L_2, V_d \rangle$, but is there any restriction on where they can be located in π? For example, the following construction in which q_1 and r_1 are constrained to lie on V_d satisfies the conditions to be a perfect two-part shared secret scheme, etc.

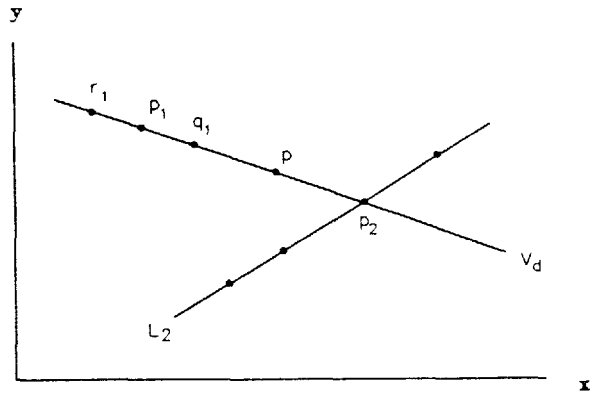


Figure 14.

However, so does the construction

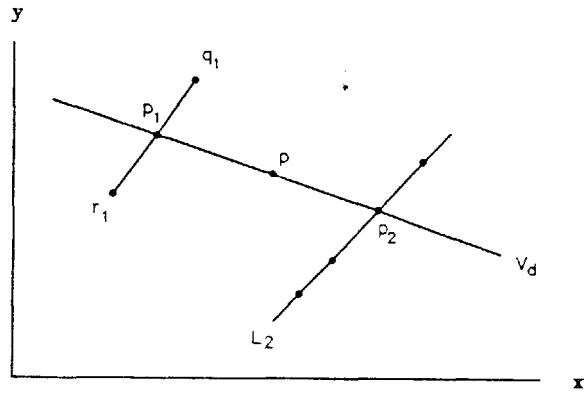


Figure 15.

In both of these constructions, the dimension of the containing space **S** is two so that it doesn't appear to make any difference where the points q_1 and r_1 are located.

On the other hand, if both parts require a 2-out-of-2 concurrence, as does the overall scheme, there is a difference:

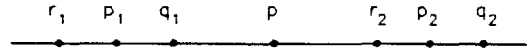


Figure 16.

versus

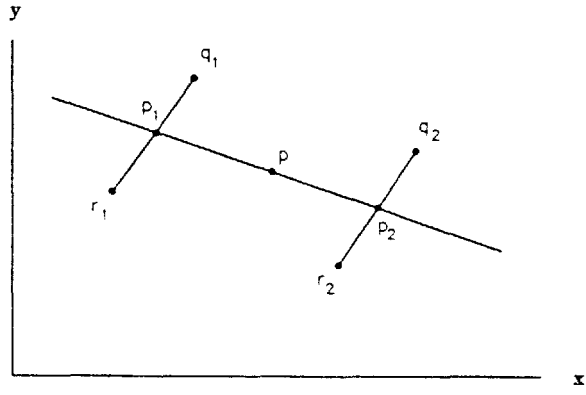


Figure 17.

The question is, which of these is the proper, i.e., logically consistent, generalization for the type of constructions we've used earlier. Increasing the number of parts from 2 to k doesn't differentiate between the two constructions either so long as the overall scheme requires unanimous agreement by the separate parts.

We consider next a three-part scheme in which the overall scheme requires the concurrence of only 2-out-of-3 parts and in which two of the parts are 2-out-of-2 schemes. The other part is a 2-out-of-ℓ scheme. In this case, a construction of the first type is given by:

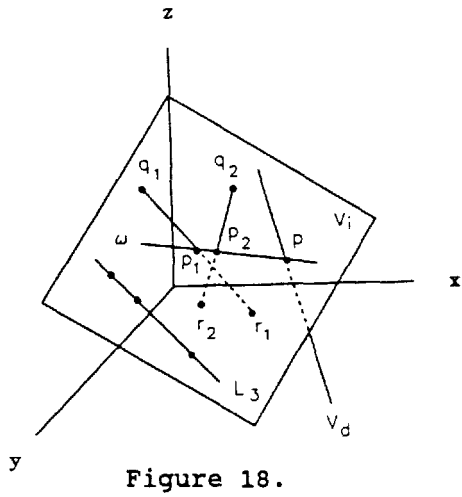


Figure 18.

where L_3 and either p_1 or p_2 determine the plane V_i and hence its point of intersection, p, with V_d. Points p_1 and p_2 determine the line ω, which lies in V_i, but which intersects V_d at p. With the same conditions on the choices for p_1 and p_2 that had to be imposed on the choice of p, in the construction of Figure 13 (and for the same reasons) this is a perfect shared secret scheme of the first type satisfying the problem specifications.

A construction of the second type is shown in Figure 19.

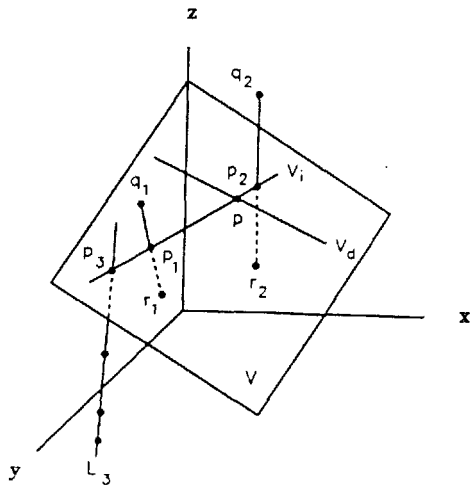


Figure 19.

V is the plane spanned by the indicator, V_i, and the domain, V_d, etc., as before. L_3 is a line outside of V which intersects V at the point p_3. The points q_1 and v_1, and q_2 and v_2 could equally well be in V or outside of V. They cannot be confined to be in V_i since if they were then a collusion consisting of any pair of points chosen from the set (p_3, q_1, r_1, q_2, r_2) would be able to determine V_i and hence p, in violation of the specified level of concurrence.

It is interesting to note that here (for this particular example) we have the first instance we have seen in which the dimensionality of the optimal constructions are the same for both types of schemes. In answer to our earlier question, the k-out-of-k control schemes should be confined to the space $V = V_i \cup V_d$, since no gain in security is achieved by letting them lie outside of this space, and one dimension (to **8**) may -- for some choices of specifications -- be saved by this restriction. We have already seen this in the degenerate case shown in Figures 16 and 17 -- degenerate because there is no V_i, so that $V = V_d$. To see this in the present case, assume that all three parts require 2-out-of-2 concurrence but that the overall scheme is 2-out-of-3. An obvious modification to L_3 in Figure 19 yields a 3-dimen-

sional solution. However a 2-dimensional solution is possible in exact analogy to the construction in Figure 16.

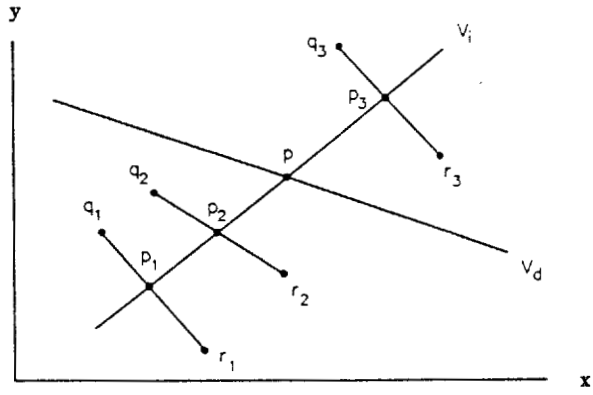


Figure 20.

It is interesting to note that in this final example the constructions are identical for both type one and type two schemes.

After all of this discussion of exceptional cases, our conclusion is the same as it was before: one cannot do better (in terms of the efficient use of information) in constructing compartmented shared secret schemes than to base them on constructions of the second type; in other words, to let the individual parts determine subindicators that point to points in a space V that define an indicator for the overall k-out-of-ℓ concurrence scheme.

An Application (and Realization) of Multilevel Shared Secret Schemes

In the brief discussion given earlier of the various extended capabilities to shared secret schemes, we described one scenario in which any two vice presidents of a bank were authorized to approve an electronic funds transfer (up to some maximum amount) or in which any three senior tellers could do so. As we remarked then, for this application it would almost certainly be unacceptable that one vice

president and two senior tellers not be able to approve a transfer. In other words, in this and many other real-world applications, a participant's ability to act must hold not only in his own class or level but in all lower-level classes as well. We remark that we are only interested in extrinsic schemes in which the worth of a particular piece of private information is totally dependent on its functional relationship to other pieces of private information, and not (in an information theoretic sense) on its own information content. Otherwise the intrinsic hierarchical schemes described earlier would be a solution to the problem, even though the amount of information a participant has to protect (keep secret) might be so great as to make the solution totally infeasible for practical application. In other words, all the pieces of private information should consist of n bits of information, even though some may be several times more effective in recovering the secret than others.

Figure 21 shows a perfect shared secret scheme for the electronic funds transfer problem.

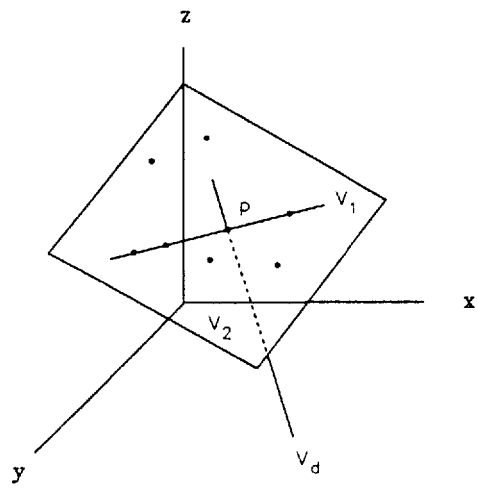


Figure 21.

Vice presidents know points on the line V_1 which intersects V_d at the point p so that any two of them can determine V_1

and hence p, etc. Senior tellers know points in general position in the plane V_2 -- not on V_1 -- and no two of which are collinear with any of the private points chosen on V_1 nor with p. Any three of them can determine V_2 and hence p, etc. Clearly any point on V_1 taken with a pair of the points in V_2 define V_2 as desired, since no such triple of points is collinear by construction.

By now the reader should be very familiar (and comfortable) with the way in which shared secret systems are constructed. For example, if we wished to conceal a 2-dimensional secret instead of a 1-dimensional secret in a 2-level scheme in which level one is a 2-out-of-ℓ scheme, we could use the same geometrical construction that was used earlier to construct a simple 3-out-of-ℓ scheme to conceal a 2-dimensional secret. Two planes, V_2 and V_d, are chosen in a 4-dimensional space such that they do not lie in a common 3-dimensional subspace. This forces them to have a single point, p, in common. In fact, we can use the same procedure used earlier to construct V_2, given V_d, so that a desired index p is the point of intersection. An arbitrary point, q, in V_2, $q \neq p$, is chosen and the line $V_1 = \langle p,q \rangle$ used to determine the points for the first class participants. The second class participants receive points in general position in V_2 none of which are on V_1 and no pair of which are collinear with either p or any point from L_1 assigned to one of the first class participants. Pictorially:

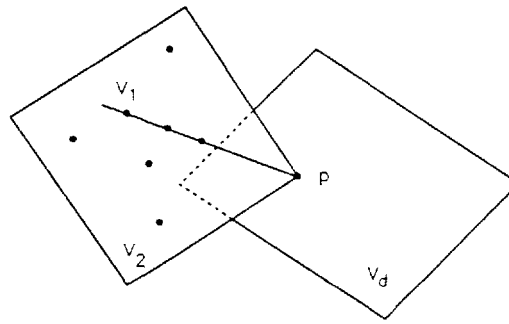


Figure 22.

An obvious extension to these constructions will accommodate an arbitrary sequence of concurrence levels, k_i, and/or a d-dimensional secret. It would appear, therefore, that this completely solves the problem of multilevel schemes.

It is only necessary to examine the construction in Figure 21 a little more critically to realize that there is more to the problem (and solution) than we have suggested. We remarked earlier that the amount of information that had to be kept secret in the private pieces of information was the same as the information contained in the secret itself. In the scheme shown in Figure 21 **S** is 3-dimensional while the secret is only 1-dimensional. One might think that in analogy to what was done with the private pieces of information in the 2-dimensional scheme shown in Figure 2 where one coordinate value was kept secret and one was exposed, that one coordinate value could be kept secret in this case as well, say z, and two exposed: $(x_j, y_j, \textcircled{z_j})$. If this is done however, the secret is revealed to even outsiders -- not just to a collusion of insiders.

Anyone knowing the nonsecret parts of the private pieces of information, i.e., their projection (along the z axis) onto the xy plane,

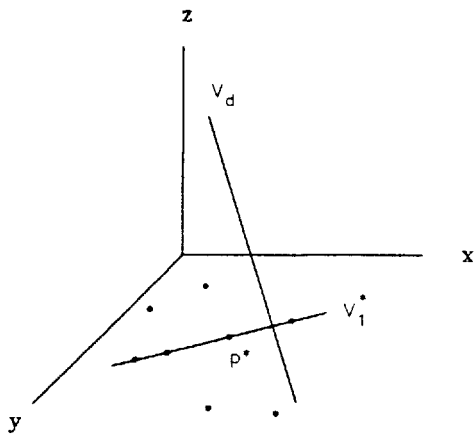


Figure 23.

also knows the projection of the line V_1 into the line V_1^*. This is easy to determine by finding any set of three or more collinear points in the projection. The line V_1 is therefore known to be in the plane π which is parallel to the z axis and includes the line V_1^*.

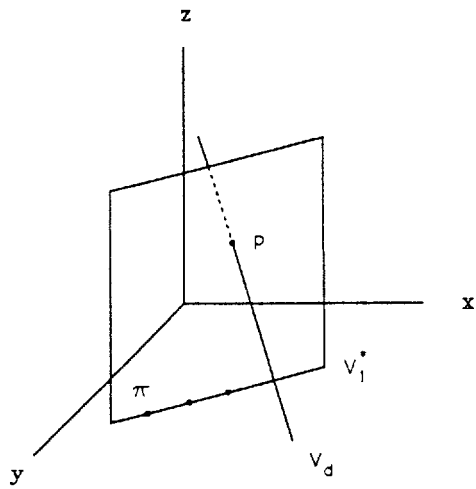


Figure 24.

In fact the unknown subvariety V_1 must be one of the pencil of lines with common point p at which the line V_d intersects π. The important point is that it isn't necessary to identify V_1, only its intersection, p, with V_d. Consequently p (and the secret) is revealed from only a knowledge of the nonsecret parts of the private pieces of information unless V_d satisfies some additional constraints. The problem goes away if the projection of V_d onto the xy plane is in the line V_1^*, in other words, if V_d is a line in π. In the extreme case V_d could be a line parallel to the z axis so that the entire line projects into a point p^* in V_1^*. p^* is the image of p under the projection along the z axis: $\text{proj}_z(p) = p^*$. V_1 and V_d are therefore distinct lines in π, at least one of which must project into the entire line V_1^*. The plane V_2 is not the same as π and in fact cannot be parallel to the z axis, hence its projection is the whole of the xy plane.

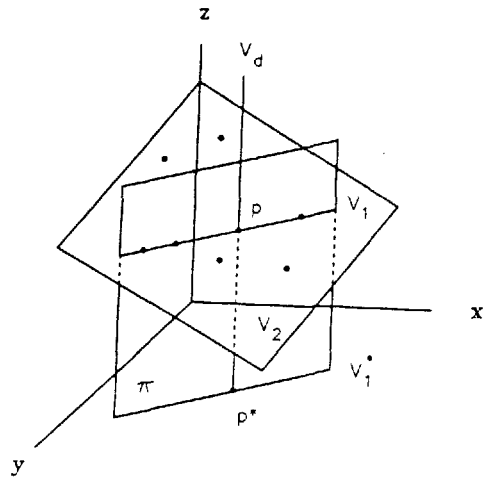


Figure 25.

In this figure V_d has been chosen to be parallel to the z axis so that p^* is the image of all of V_d and hence known. Otherwise the projection of V_d is all of V_1^* and the projection of p, p^*, would be unknown.

The problem that we encountered in partitioning the private information into a secret part and a nonsecret part for the multilevel scheme shown in Figure 21 without compromising the security of the secret is common to almost all multilevel schemes. The solution for that particular case, while suggestive of the general method of solution, is not definitive. To better illustrate the general case, we next consider the two-level scheme shown in Figure 22. $\mathbf{S}$ was 4-dimensional in that case and the secret was 2-dimensional so that the private information would be (if the previous examples are any guide) of the form $(x_j, y_j, \textcircled{z_j}, \textcircled{w_j})$. The line V_1 projects into a line V_1^* in the xy plane. In this case, corresponding to the plane π that was defined on V_1^* in the construction in Figure 24, there is a 3-space, S, parallel to the z and w axes which includes the line V_1^*. Since $\mathbf{S}$ is only 4-dimensional, the plane V_d either intersects S in a line or else contains S. By the rank formula, $\mathbf{S}$ would have to be 6-dimensional for the two subspaces to be

skew and 5-dimensional for them to intersect in only a point. If $S \cap V_d = \ell$, ℓ a line, then the scheme cannot be perfect since the equivocation about the secret would be only of $0(q)$ instead of $0(q^2)$ using the exposed (nonsecret) parts of the private pieces of information. It must therefore be the case that $V_d \subset S$. This does not say that

$$\text{proj}_{z,w}(V_d) = \text{proj}_{z,w}(V_1)$$

but merely that

$$\text{proj}_{z,w}(V_d) \subset \text{proj}_{z,w}(V_1) \quad .$$

This is analogous to the previous case in which $\text{proj}_z(V_d)$ was either the point p^* (in the line L_1^*) or else all of L_1^*.

Although it is possible to formulate general conditions on the subspaces which will insure that these problems are avoided -- even if the subspaces are chosen almost at random -- there is no gain in security nor a compensating increase in capability to justify this additional freedom of choice. Instead, in the first example we may as well take V_d to be a line parallel to the z axis so that $\text{proj}_z(V_d) = p^*$, $p^* \in V_1^*$, and in the second to take V_d to be parallel to the z and w axes so that $\text{proj}_{z,w}(V_d) = p^*$, $p^* \in \text{proj}_{z,w}(V_1) = V_1^*$ in this case also. If we construct the domain V_d in this manner, the secret part of the private information will be totally lost in the projection, i.e., in the disclosure of the nonsecret part, and the scheme will be secure.

Finally, given a d-dimensional secret which is to be secured in a t-level scheme, where the concurrence required at level j is k_j,

$$k_t > k_{t-1} > \ldots > k_1 \quad ,$$

and in which a participant at the j-th level is to be able to function at all lower levels (having however only the

capability associated with that level) we can construct a perfect multilevel control scheme with these characteristics. We start with an n-dimensional space, $\mathcal{S} = PG(n,q)$, where $n = d+k_t-1$. V_d is a d-dimensional subspace of $\mathcal{S}$ parallel to the coordinates $x_d, x_{d-1}, \ldots, x_1$. Given the secret point p in V_d, we construct a (k_t-1)-dimensional subspace, V_t, of $\mathcal{S}$ that intersects V_d only in the point p. We next choose a $(k_{t-1}-1)$-dimensional subspace V_{t-1} of V_t lying on the point p. This procedure is repeated to finally yield a chain of nested subspaces

$$V_t \supset V_{t-1} \supset \ldots \supset V_1$$

of dimensions $k_t-1, k_{t-1}-1, \ldots, k_1-1$, respectively, all of which lie on the point p.

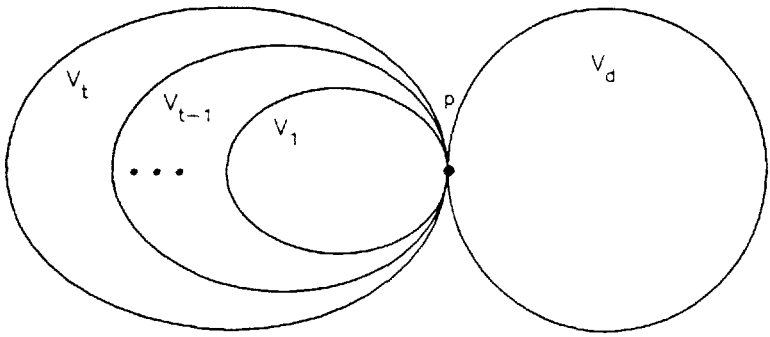


Figure 26.

The private pieces of information are to be chosen so as to have rank k_j in V_j and to not lie in any of the higher order subspaces. In other words, in the construction shown in Figure 21, the points in V_2 were chosen not to lie on V_1 and such that no two were collinear with any of the private points chosen on V_1 nor with the index, p. In general, this says that the points in the j-th class are to be chosen in general position in $V_j \setminus \bigcup_{i=1}^{j-1} V_i$, such that the rank of any set of k_j points drawn from among all of the private points in $\bigcup_{i=1}^{j} V_i$ and the index, p, will be k_j. Under these conditions

clearly any participant can act as a member of any lower class. The private information will be of the form

$$(x_n,\ldots,x_{d+1},\textcircled{x_d},\ldots,\textcircled{x_2},\textcircled{x_1})$$

and the scheme will be perfect since the secret information is totally lost in the projection along the first d coordinates.

Conclusion

In view of the length of this paper we merely remark in conclusion that the two types of partitioning of secret information which have been described here can be combined to form hybrid control schemes involving simple, multipart and multilevel controls. For example, it would be easy to devise a two-part control scheme in which both the U.S. military command and the U.S.S.R. military command had to concur in order for the controlled event to be initiated. The U. S. could choose to use a multilevel scheme, say one in which two or more generals, three or more colonels (or generals) five or more lieutenent colonels (or colonels or generals) had to concur in order for the U. S. input to be made. The U.S.S.R. on the other hand might have entirely different requirements; for example they might require the unanimous concurrence of three of their general staff in order for the U.S.S.R. input to be made. The constructions described here are sufficiently general to accommodate both arbitrary concurrence of the parties and arbitrary multi-level concurrence within the individual parts. There are concurrence schemes, however, that can't be satisfied by schemes of the type described here, but it appears unlikely that any such scheme will be of practical interest: one such example would be if participants A and B together could cause an event to be initiated but A, B and C together could not.

Bibliography

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

[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, April 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, March 1983, pp. 208-210.

[3.] 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.

*[4.] A. Beutelspacher and K. Vedder, "Geometric Structures as Threshold Schemes," Proceedings of the 1987 IMA Conference on Cryptography and Coding Theory. Cirencester, England, Oxford University Press, to appear.

[5.] 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.

[6.] 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 CryptolocrY$_r$ Vol. 263, Ed. by A. M. Odlyzko, Springer-Verlag, Berlin, 1986, pp. 266-274.

[7.] 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.

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

[9.] 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, April 14-16, 1980, pp. 108-113.

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

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

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

[13.] E. F. Brickell and D. R. Stinson, "The Detection of Cheaters in Threshold Schemes," preprint (available from authors).

[14.] 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.

[15.] 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.

[16.] 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, University of California, Berkeley, 1982.

[17.] 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.

[18.] 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, April 14-16, 1980, pp. 100-102.

*[19.] M. De Soete and K. Vedder, "Some New Classes of Geometric Threshold Schemes," Proc. Eurocrypt'88, May 25-27, 1988, Davos, Switzerland, to appear.

*[20.] A. Ecker, "Tactical Configurations and Threshold Schemes," preprint (available from author).

[21.] Paul Feldman, "A Practical Scheme for Non-interactive 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.

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

*[23.] 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).

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

*[25.] 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, February 9-12, 1981, IEEE Trans. Info. Theory, Vol. IT-29, No. 1, January 1983, pp. 35-41.

*[26.] 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.

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

*[28.] R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes," Com. ACM, Vol. 24, No. 9, September 1981, pp. 583-584.

[29.] 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.

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

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

*[32.] 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, November 1979, pp. 612-613.

*[33.] 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.

*[34.] 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.)

*[35.] D. R. Stinson, "Threshold Schemes from Combinatorial Designs," submitted to the Journal of Combinatorial Mathematics and Combinatorial Computing.

[36.] 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.

*[37.] 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 December 1988.

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

*[39.] 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) English translation available from G. J. Simmons.

[40.] H. Yamamoto, "Secret Sharing System Using (k,L,n) Threshold Scheme," Electronics and Communications in Japan, Part 1, Vol. 69, No. 9, 1986, pp. 46-54; translated from Tsushin Denshi Gakkai Ronbunshi Vol. 68-A, No. 9, Sept. 1985, pp. 945-952.

*[41.] 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.