CHAPTER 9

An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*

G. J. SIMMONS
Sandia National Laboratories
Albuquerque, New Mexico 87185

*This work was performed at Sandia National Laboratories and supported by the U.S. Department of Energy under contract number DE-AC04-76DP00789.

It may seem odd to have a chapter on secret sharing appear in a volume devoted to cryptology, but as we shall see, secret sharing is intimately related to two problems common to all cryptosystems, namely, the problems of key management and key distribution. The justification for this chapter, however, is even more direct since the larger subject of this volume is how to insure that information-based systems either cannot be caused to function improperly through tampering with the information they act on, or else to detect (in probability) if they have been caused to function improperly by such tampering. The integrity of information (from unauthorized scrutiny or disclosure, manipulation or alteration, forgery, transmission, false dating, etc.) is commonly provided for by requiring operation(s) on it that one or more of the participants or elements in the system, who have access to 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 have access to the private information.

Encryption/decryption in a single cryptoalgorithm is a paradigm of such an operation, with the common key being the private (secret) piece of information. If the transmitter can rely on the receiver protecting and keeping secret his copy of the key, then he—the transmitter—can be confident that he can communicate information to the receiver in private, that is, with secrecy. Conversely, if the receiver can rely on the transmitter keeping his copy of the key secret, then he—the receiver—can be confident that the ciphers he receives and decrypts into acceptable messages must have been sent by the (legitimate) transmitter. Although it is implicit in single-key cryptosystems, it is almost never stated explicitly that the transmitter and the receiver must unconditionally trust each other since either can do anything that the other can. What this means is that the receiver could falsely claim to have received an encrypted message from the

transmitter that the transmitter would be unable to prove (to an impartial third party or arbiter) that he hadn't sent. Conversely, the transmitter could send an encrypted message to the receiver and then disavow having sent it and the receiver would likewise be unable to prove that he hadn't generated the encrypted message himself. In this case the transmitter must unconditionally trust the receiver to not falsely attribute messages to him that he did not send, and the receiver must unconditionally trust the transmitter to not disavow messages that he did send. There are situations in which the participants are all willing to unconditionally trust each other, but there are many more in which they are not.

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, and hence to trust the system function, even though they may not trust all of the elements. A paradigm for such a protocol is the cryptographic key distribution system described in American National Standards Institute (ANSI) X9.17 [R1] which makes it possible for 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). In reality, however, there is generally no unconditionally trustworthy element—be it a person or a device—only elements of tolerable trustworthiness, or circumstances that compel them to be accepted as trustworthy as in the case of customers' acceptance of the security of automated teller machines (ATMs), and of user identification via personal identification numbers (PINs).

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, that is, 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 at any given time there are some (unidentified) elements in the system that 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—on the assumption that the more elements that must collude or be compromised in order for a deception to be possible, or to go undetected, the less likely the deception is to occur or to escape detection if it does occur. To protect against random failures of devices, say in fault-tolerant networks, this task 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 that the United States enforces for critical military actions. This is the simplest possible example of secret sharing or shared control since in this case there are only two parties, each of whom knows a private piece of information that when combined with the piece known only to the other party suffices to allow access to (or control of) a weapons system, but each of which individually provides its holder no greater chance of access or ability to use the weapon than what an outsider who knows nothing at all about the secret controlling information would have.

In this chapter, we will develop the general principles of secret sharing and/or shared control as a means for increasing the confidence in the proper functioning of information-based systems and examine a number of the characteristics such systems need to have for various real-world applications over and above the simple property of enforcing the concurrence of a predesignated number of the participants before a secret piece of information can be recovered or a jointly controlled event initiated. These schemes are all 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 controlling secret information.

1 INTRODUCTION

In 1979, Blakley [10] and Shamir [53] independently devised shared secret schemes for the same application: robust key management for cryptosystems. They were concerned both with the problem of legitimate users being locked out of the system, that is, of the key being lost for some reason, and of unauthorized users getting in. Although their approaches to solving these problems were quite different, as we shall see in a moment, the essential notion is the same in both cases. Given a cryptographic key, that is, the secret piece of information, one wishes to construct ℓ related pieces of information with the property that any set of k of these pieces will suffice to recover the original secret, but such that no subset of $k - 1$ or fewer of them will reveal it. Given such a construction, the pieces of information can then be distributed privately and securely to the ℓ participants in the secret sharing scheme. If there are ℓ of the private pieces of information (generally called "shares" by those authors whose work derives from Shamir's or "shadows" by those who use Blakley's model) and k are required to reconstruct the secret, the scheme is called either a k-out-of-ℓ shared secret scheme or a (k, ℓ)-threshold scheme, respectively. Thereafter, as many as $\ell - k$ of the private pieces of information could be lost or unavailable when needed and the key could still be reconstituted, while no security breach of fewer than k of the pieces could reveal the key to an unauthorized user.

Since we will generalize the notion of shared control (of information and hence of actions dependent on that information) in ways that cannot be easily viewed as threshold schemes, we will use the term shared secret scheme since this emphasizes the essential feature of shared capability as opposed to the more restrictive notion of simply requiring the concurrence of a specified number of the participants. Both the Blakley and the Shamir constructions realize k-out-of-ℓ shared secret schemes, however, as we have already mentioned their constructions are fundamentally different. We will first describe their schemes in detail and then make use of these differences to illustrate several concepts important to shared secret and/or shared control schemes in general.

Shamir's construction is the easier to explain and is algebraic in nature—based on interpolation of a polynomial defined over a finite field, $GF(q)$. Figure 1 illustrates the basic idea. Given k points in the two-dimensional plane, (x_i, y_i) $i = 1, 2, \ldots, k$, there is a unique $(k - 1)$st degree polynomial, $\mathbf{P}^{k-1}(x)$, for which $\mathbf{P}^{k-1}(x_i) = y_i$ for all i. If the secret (key) is taken to be an element $p \in GF(q)$, it can be partitioned into ℓ shares

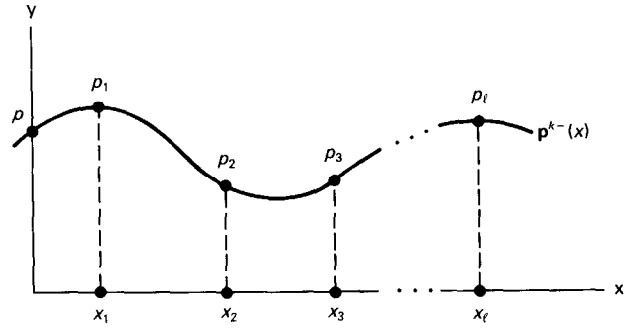

Figure 1

as follows. A $(k-1)$st degree polynomial $\mathbf{P}^{k-1}(x)$ is chosen randomly. $\mathbf{P}^{k-1}(x)$ has the representation

$$\mathbf{P}^{k-1}(x) = \sum_{i=0}^{k-1} a_i x^i \tag{1}$$

where the constant term a_0 is the secret p; that is, $\mathbf{P}^{k-1}(0) = a_0 = p$. The ℓ shares, $p_i = (x_i, y_i)$, $\ell \geq k$, are calculated by evaluating Eq. (1) at ℓ distinct points x_i, $x_i \neq 0$:

$$p_i = y_i = \mathbf{P}^{k-1}(x_i) \tag{2}$$

Given any subset of k of these points, it is computationally easy using Lagrange interpolation to solve for $a_0 = p$ in Eq. (1), that is, to recover the secret. Given only $k' \leq k-1$ of the private pieces of information (points on $\mathbf{P}^{k-1}(x)$) a_0 could equally likely be any element in $GF(q)$ since for each choice of a point p' on the y-axis there will be equally many $(k-1)$st degree polynomials through the subset of k' points and p'. Consequently, any collusion of fewer than k of the participants (the insiders) will have no better chance of determining the secret than will an outsider who has no privileged information at all. To all unauthorized groupings (fewer than k participants) including outsiders, the secret is equally likely to be any point on the line $(0, y)$, that is, the probability of guessing p will be $1/q$. A shared secret scheme in which insiders (and all unauthorized groupings of insiders) have no advantage over outsiders in guessing the secret are said to be *perfect*. Shamir's polynomial interpolation shared secret scheme is perfect in this sense.

The private information content of each share in a perfect shared secret must be at least as great as the information content (equivocation) of the secret itself. This is easy to see. Assume that some share has less private information in it than does the secret, and consider an arbitrary collusion of $k-1$ participants not including the deficient share. Since the system is perfect, the $k-1$ of them together are, by definition, equally uncertain of the secret as an outsider. On the other hand, if they knew the missing (deficient) share they could recover the secret, since they are all participants in a k-out-of-ℓ shared secret scheme, but their uncertainty about the missing share value is less than their uncertainty about the secret: a contradiction. Therefore, the private in-

formation content in each share in a perfect secret sharing scheme is necessarily at least as great as the uncertainty (information content) of the secret itself. If equality holds, the shared secret scheme is said to be *ideal*. As described, Shamir's scheme is not ideal since each private point consists of a pair of coordinate values, that is, two elements in $GF(q)$, whereas the secret is a single element in $GF(q)$. This is not an essential difference, however, and we will return to this point below. For the moment we only wish to introduce and define the concept of ideal shared secret schemes.

Shamir recognized that it might be desirable in some circumstances for participants to have differing capabilities to recover the secret. He proposed to accomplish this by giving more than one point on the polynomial $\mathbf{P}^{k-1}(x)$ to the more capable participants. If $k = 4$, so that four points are required to recover $\mathbf{P}^3(x)$ then by giving pairs of points to participants in Class I and single points to participants in Class II a scheme could be set up in which any subset that included two participants from Class I or four participants from Class II or one participant from Class I and any two from Class II would be able to recover the secret, while any collection of participants and outsiders that did not satisfy one of these conditions would be unable to do so. Schemes of this sort in which the differing capability of the participants private pieces of information to assist in the recovery of the secret are a function of their information content we define as *intrinsic*. An intrinsic scheme with more than a single class of capability cannot be perfect.

The converse to an intrinsic scheme is an *extrinsic* one wherein the differing capability of the private pieces of information to assist in the recovery of the secret are a consequence of their functional relationship to the other private pieces of information, not on their differing information contents. An ideal scheme is necessarily an extrinsic one, but an extrinsic scheme may not be ideal since the private pieces of information, while they all contain the same amount of information, may all contain more bits of information than are in the concealed secret. Brickell and Davenport [19] have introduced the terminology of *strongly ideal* shared secret schemes for those in which the secret point and the private pieces of information are each drawn from the same space with the same probability distribution, that is, in which all of the points in some geometric object are equally likely to be the secret as they are to be a private piece of information. We will have to wait until later to exhibit convincing examples of extrinsic schemes since we aren't yet ready to deal with differing capabilities for the participants. We will also show how to realize arbitrarily complex but perfect shared secret schemes. For the time being, though, these are the only properties of shared secret schemes we wish to point out using the Shamir constructions.

Blakley's construction for shared secret schemes is geometric. To motivate his terminology of "shadows" for the private pieces of information, consider the construction shown in Fig. 2.The secret (information) in this case is the point p in the three-dimensional space E^3. p has been projected (along the x-axis) from infinity to generate the "shadow," p_{yz}, of p in the plane yz. Similarly, p is projected parallel to the y- and to the z-axes to generate the shadows p_{xz} and p_{xy}, respectively. The private pieces of information in this case are the three shadows p_{xy}, p_{xz}, and p_{yz}. The resulting scheme is a (2, 3)-threshold scheme. It should be mentioned that this is not precisely the way Blakley uses the term "shadow," although it is equivalent. We will give his general definition shortly, after the concept is made intuitively clear. Participant i, $i = x$, y, or z, knows that his shadow is the result of projecting the point p parallel to the i-axis, that

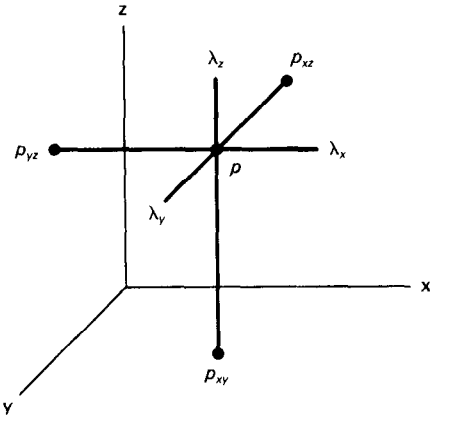

Figure 2

is, he knows that p is a point on the line λ_i through his shadow (private point) and parallel to the i-axis. Since the three lines, λ_i, all intersect in the point p, any two of them suffice to determine it. Any one of the participants alone, however, knows only that p is a point on a line that he (alone) knows.

This small example already suffices to illustrate an important characteristic of Blakley's construction for shared secret schemes—subsets of $k - 1$ or fewer participants (the insiders), including individual participants, have an advantage over outsiders in guessing at the secret information because of their knowledge of the private information. The setting for Blakley's shared secret schemes is not in a Euclidean space E^n, but rather in a finite projective space $PG(n, q)$, but more importantly, his construction of the shadows is slightly less intuitive than what we have done in the small 2-out-of-3 scheme. Continuing with this example for the moment, in Blakley's setting the space would be $PG(3, q)$, in which there are $q + 1$ points on a line and $q^3 + q^2 + q + 1$ points in all. An outsider's chances of guessing p (assuming, of course, that p was chosen originally with a uniform probability distribution on the points in $PG(3, q)$) would be $(q - 1)/(q^4 - 1) \approx 0(q^{-3})$, while the probability of any one of the participants guessing p would be $(q - 1)/(q^2 - 1) \approx 0(q^{-1})$. Consequently, this example—and the Blakley shared secret scheme in general—is not perfect.

There isn't anything special about the choice of the three lines λ_x, λ_y, and λ_z in Fig. 2 to be parallel to the x-, y-, and z-axes, respectively. This choice was made to simplify the example. In the projective space, $PG(3, q)$, there are no parallel lines, but the projectors of p could equally well have been any other three distinct lines lying on the point p. When looked at in this generality, if p is a finite point of $PG(3, q)$, then the $q^2 + q + 1$ lines lying on p are simply the projectors of p from each of the $q^2 + q + 1$ points in the plane at infinity, that is, the lines defined by p and the points in the plane at infinity. Any pair of these lines intersect in the point, p, and hence the lines can be used as the private pieces of information in a 2-of-ℓ shared secret scheme; $\ell \leq q^2 + q + 1$.

In complete generality, the private pieces of information can be considered to be the projection of the point p from a (private) point in one plane, π_1, onto another plane, π_2, that is, the shadow of p in π_2 under such a projection. p cannot be a point in the plane π_1 which is why in the example we choose p to be any finite point and π_1 to be

the plane at infinity. We have described this construction in such tedious detail to motivate Blakley's terminology for the private shares as "shadows." If one takes not points in the plane at infinity, but lines in the plane, then the geometric objects defined by these lines and p would be all of the planes on p in $PG(3, q)$. In this case any three of the planes not on a common line through p would define p by their intersection. In general, k randomly chosen hyperplanes—$(k - 1)$-dimensional subspaces in PG(k, q)—will probably define, that is, intersect in, a single point.

Blakley's construction for a k-out-of-ℓ shared secret scheme makes use of this simple geometric result. The secret, p, is a randomly chosen point in $PG(k, q)$. The ℓ shadows are chosen from among the $(q^k - 1)/(q - 1)$ hyperplanes (subspaces of projective dimension $k - 1$) lying on p. If q is sufficiently large and ℓ is not too large, the probability of any subset of k of these shadows having more than one point in common is very close to zero. If this statistical confidence isn't adequate, as Blakley points out, it is an easy matter to test to insure that this independence condition is satisfied by the chosen set of shadows. Blakley's construction in $PG(3, q)$ would therefore not be a set of lines, λ_i, on p, but rather a set of hyperplanes, π_i on p defining a 3-out-of-ℓ threshold scheme as shown in Fig. 3.

There are $q^2 + q + 1$ such planes (on the point p) so that any ℓ, $3 \leq \ell \leq q^2 + q + 1$, is possible for a 3-out-of-ℓ scheme in such a construction. As already remarked, this is not a perfect scheme since outsiders can only guess at p being a point in $PG(3, q)$ while any insider has only to guess at p being a point on the plane (shadow) that he knows. The reader can now appreciate why we developed the Blakley implementation of shared secret schemes in the way we did, since the planes in Fig. 3 are not suggestive of "shadows" of p, while the points p_{ij}, $i \neq j$, in Fig. 2 are.

Blakley's shared secret schemes are, in general, far from ideal since each participant must have enough private information to identify his shadow (a $k - 1$)-dimensional hyperplane). This requires k coordinate values, that is, k elements from

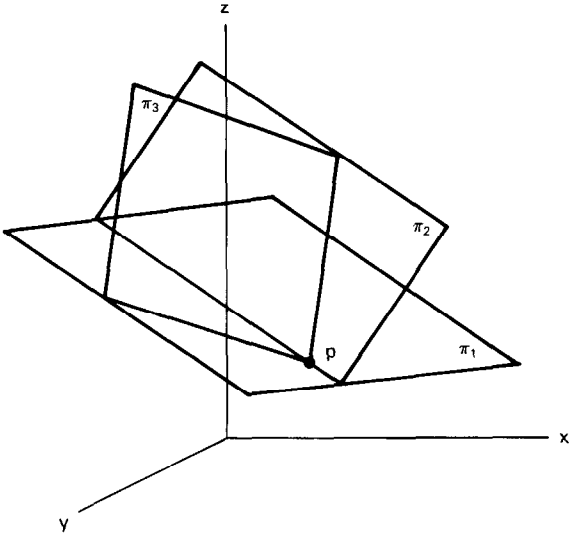

Figure 3

$GF(q)$. On the other hand, a collusion of $(k - 1)$ participants can only have linear uncertainty about the secret since their $(k - 1)$ hyperplanes intersect in a line that must include the secret point p. This means that there is precisely one coordinate value of uncertainty, that is, 1 out of $q + 1$ equally likely values, for the secret—in the worst case of an improper collusion of $k - 1$ of the participants—while each participant is responsible for k, $k \geq 2$, elements from $GF(q)$ as his private information.

The reason for describing the shared secret schemes of Shamir and of Blakley at such great length is not purely historical. As we shall see in the next section, their constructions typify two fundamentally different, but general, approaches to shared secret schemes, both of which we will need to generalize and understand for later application. We should point out that a modest literature (at least the over 60 papers cited in the Bibliography on shared secret schemes at the end of this chapter) has been generated since the notion was first discovered by Shamir and Blakley. However, since all of the schemes proposed thus far are subsumed in the general models given in the next section, and since the purpose of this chapter is to provide a tutorial introduction to shared secret and/or shared control schemes, we will not attempt a survey of the literature. As a partial compensation for this, the bibliography includes every paper on the subject known to the author—not just the ones cited as references here.

2 THE GENERAL MODEL(S)

There are two essentially different ways in which pieces of information related to another, secret, piece of information can be constructed and distributed among a group of participants so that designated subsets of the participants will be able to recover the secret piece of information, while no collection of participants that doesn't include one of these subsets can. As it happens, the schemes discovered by Shamir and Blakley provide ready examples for each of these classes of shared secret schemes. In some schemes, the set of possible values for the secret, consistent with all of the private pieces of information that have been exposed, remains unchanged until the last required piece of private information becomes available, at which point the unique value for the secret suddenly becomes the only possibility, as was the case for the Shamir construction. In others, as each successive piece of the private information is exposed, the range of possible values that the secret could assume narrows, until finally when the last required piece of private information becomes available, the secret will have been isolated and identified as was the case for the Blakley construction. There are numerous examples of each type of system and applications in which the most natural solution involves an intermixing of the two.

We begin our development of the general models with a discussion designed to clarify the essential difference between the two classes of schemes. Without loss of generality, the secret can always be considered to be a point, p, in some suitably chosen space. The function of a shared secret scheme is to make it possible for authorized subsets of the participants to identify this point, but to make it improbable that any collection of participants and/or outsiders that doesn't include an authorized subset of the participants can do so. We have seen that the constructions of both Shamir and of Blakley satisfy these conditions when the authorized subsets are defined by a simple threshold condition; that is, that k or more (out of ℓ) of the participants must concur before the secret can be reconstituted or the controlled action initiated. This includes the special case of unanimous consent, $k = \ell$.

In real-world applications, however, the concurrences that one needs to be able to insure exist before the shared control can be initiated may be much more complex: For example, a bank might want to require the concurrence of two vice-presidents or of three senior tellers for it to be possible to authenticate an electronic funds transfer (EFT)—with the natural requirement that a vice-president should also be able to act in the stead of a senior teller, that is, that any vice-president and any two senior tellers should also be able to authenticate an EFT. To realize these more general concurrence schemes (or access structures in the terminology of Benaloh and Leichter [3], Brickell and Davenport [19], or Brickell and Stinson [20]), the model for shared secret schemes must be much extended. Since the discussion of these extensions will (unavoidably) be both lengthy and detailed, the reader may find it helpful to know in advance approximately what we are going to do.

In Shamir's threshold scheme, each participant holds as his private piece of information a point on a polynomial $\mathbf{P}^{k-1}(x)$ which can be thought of as a geometric object—in this case the function $y = \mathbf{P}^{k-1}(x)$—that "points" to the secret point, p, on the y-axis. In a strict sense, $\mathbf{P}^{k-1}(x)$ is "spanned" by any k of the private pieces of information. We will generalize this notion so that a geometric object (usually an m-dimensional subspace of the containing space $\mathbf{S}$) spanned by the set of private points held by each of the authorized concurrences of participants will point to the secret point, p, in some other geometric object, also usually a subspace of S. Most of our constructions will be of this simple form, although the geometry of the two objects involved may be exceedingly complex.

In Blakley's scheme, each participant holds, as his private piece of information, a geometric object—actually a hyperplane in his construction, but we want to deliberately suggest a more general construction—that he knows contains the secret point p. In a simple threshold scheme, the objects are chosen so that any subset of k of them will intersect in, that is, identify, the unique point p. If this approach to shared secret schemes were generalized, one would require that each collection of the geometric objects (private pieces of information) held by one of the authorized concurrences of participants should also unambiguously identify p by their intersection. We will not pursue the generalization of Blakley-type shared secret schemes, however, since these schemes can never be perfect, because as the number of participants in a collusion increases, the uncertainty about the secret, p, must decrease since p is in each of the privately held geometric objects and hence in their intersection as well.

Consider the simplest possible example of a shared secret scheme, a 2-out-of-ℓ scheme. A generalized version of the Shamir construction for this case is shown in Fig. 4. We say generalized because the secret is no longer the constant term of the shared polynomial, that is, the intersection of the curve $y = \mathbf{P}^{k-1}(x)$ with the y-axis, but rather the point of intersection of two subspaces—lines in this case.

The private pieces of information are points on a line V_i, whose intersection with a line V_d is the index point, p, at which the shared secret information is defined: $p = (x_p, y_p)$. We call the reader's attention to an important change in terminology that has been introduced here. In Shamir's paper and in our discussion of his construction, the secret was defined to be a (randomly chosen) point in the ground field, $p \in GF(q)$. Similarly, the constant term, a_0, of the polynomial $\mathbf{P}^{k-1}(x)$ was equally likely to be any element of $GF(q)$ since $\mathbf{P}^{k-1}(x)$ was randomly chosen from all of the $(k-1)$-st degree polynomials over $GF(q)$. This made it natural to equate p with a_0. In the construction of Fig. 4, p is a point on the (publicly known) line V_i. However, since p satisfies a known

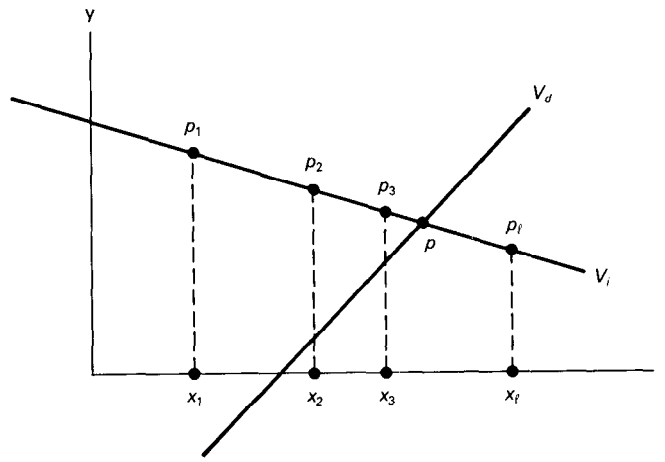

Figure 4

linear constraint there is only one degree of freedom, that is, of uncertainty, to it. In other words, the uncertainty about p is only $H(p) = \log_2(q)$ bits—in the affine plane $AG(2, q)$—just as it was for the Shamir construction. We assume that some entropy-preserving function is evaluated at p to recover the secret. One suitable function would be the projection of p onto the y-axis, which, of course, is identical with the Shamir construction when V_d is the y-axis. There are many such entropy-preserving transformations, which as we will see later is an essential characteristic of this construction for shared secret schemes.

As we have pointed out elsewhere [55] and will discuss in detail below, the information needed to specify the points, p_i, is not all of the same type insofar as its security requirements are concerned. If we use the obvious specification of the point p_i in the affine plane $AG(2, q)$ by its coordinates (x_i, y_i), then it is sufficient (for the security of the shared secret scheme in this example) that each participant keep secret one of the coordinate values (say y_i), and that he merely insure the integrity of the other coordinate value against substitution, modifications, etc. With this convention for partitioning the private pieces of information into secret and nonsecret parts, V_i cannot be parallel in the affine plane to the y-axis since in that case the nonsecret parts would all be the same, $x_i = x_p$ for all i, and V_i itself, and hence p, could be deduced from the exposed (nonsecret) parts of any pair of private pieces of information.

The point we wish to make using this simple scheme has to do with the probability of some improper (i.e., unauthorized) collection of persons recovering the secret. An outsider who knows only the geometric nature of the scheme, that is, the line V_d and that there is a line V_i whose intersection with V_d determines the unknown point p and the public parts of the private pieces of information, cannot restrict the possible values for p beyond the fact that it is a point on V_d. Since each of the q points of V_d has the same number of lines on it that are not parallel to the y-axis and hence could be the unknown line V_i, it should be obvious that the opponent can be held to an uncertainty about the secret of

$$H(p) = \log(q) \tag{3}$$

that is, his "guessing probability" of choosing p in a random drawing using a uniform probability distribution on the points of V_d. This is the best (security) that can be achieved by any scheme for concealing p.

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

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

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

We next consider the Blakley construction for a 2-out-of-ℓ shared secret scheme shown in Fig. 5. In this case, the private pieces of information are lines all of which are concurrent on the secret point p. To an outsider, every point in the plane is equally likely to be the point p, hence his uncertainty about p is

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

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

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

Consequently, this scheme is not perfect, since the insiders have an advantage (in cheating) over an outsider. Both schemes, however, provide the same minimum level of security against unauthorized recovery of the secret information. From that standpoint alone, they would appear to be equally good. There are other factors that need to be considered, such as the amount of secret information each participant must be responsible for—or even the information content of the part whose integrity must be

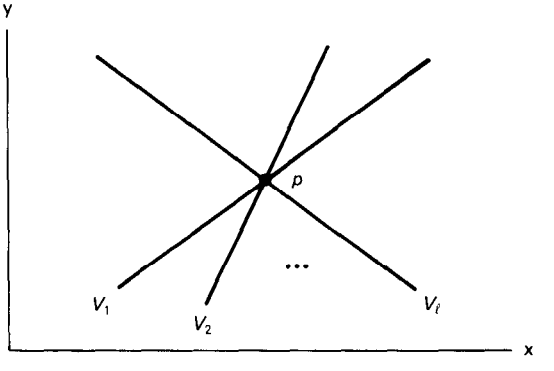

Figure 5

insured—and the information content of the secret itself. Since the plane is two-dimensional in both points and lines, it is easy to see that in either example the participant need only keep the equivalent of one coordinate value, that is, $\log(q)$ bits, secret about his private piece of information and to insure the integrity of a like amount of information. Thus, the two schemes are equivalent with respect to these parameters. It is at least plausible to measure the security of a shared secret scheme by the least uncertainty faced by any unauthorized person or grouping of persons about the secret; in other words, $\log(q)$ bits in both examples as well.

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

In the first example, where the secret was defined at the point p on the line V_d, the security of the scheme was measured by the uncertainty about p, which, as we saw, was the same for an outsider or for any one insider. We now examine this example from a different standpoint. Although it may seem strange at first to do so, the line V_i can be thought of as being a cryptographic key that encrypts the plaintext (ordinate) of a private piece of information into the ciphertext (abscissa). This is consistent with our convention that the ordinate is the information being protected (kept secret) and that the abscissa can be exposed. The secret information is the decryption of a known ciphertext (the ordinate, x_p, of the point p) using the key V_i. In this simple geometric construction of a 2-out-of-ℓ shared secret scheme if V_i is to define a cryptotransformation, it must not be parallel to either the y-axis or the x-axis in order for it to define a one-to-one mapping (i.e., a nonsingular linear transformation) of the y-axis onto the x-axis.

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

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

$$H(V_i) = \log(q^2) = 2\log(q) \tag{7}$$

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

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

$$H(p) = \log(q) \tag{8}$$

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

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

$$H(V_i) = H(p) = \log(q) \tag{9}$$

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

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

The examples shown in Figs. 4 and 5 contain all of the essential features for the general models we will use for the two types of shared control schemes, irrespective of how complex the required concurrence may be or of what other properties the shared

secret scheme may be required to have. In the first type of scheme, there is one geometric object (an algebraic variety, generally a linear subspace in some higher dimensional space), which can be determined given any subset of the points in it that includes at least one of the specified concurrence groupings, which intersects another object in a single point, p, at which the secret is defined. While p is a point in both of the sets, the first set is always secret (until it is reconstructed by an authorized concurrence among the participants) while in many applications the other is publicly known, a priori. We therefore refer to the geometric object (set of points) whose determination isn't shared among the participants as the domain variety, V_d, since the secret (argument) can be thought of as being a point concealed in its domain. The object determined by the shared information can be thought of as indicating (in the sense of pointing to) the secret point p in V_d. We therefore call this object the indicator (variety), V_i. Stripped of the inessential (to the present discussion) details of how sets of points can be chosen in a variety V_i so that any of the designated subsets of them will suffice to reconstruct all of V_i, the configurations of interest are of the form shown in Fig. 6.:

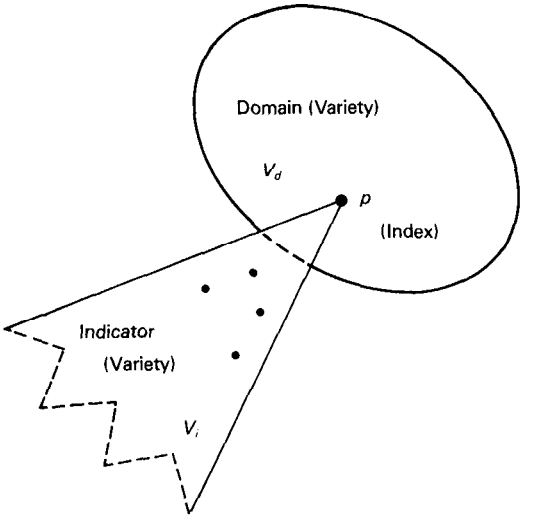

Figure 6

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

A single shared secret scheme may have either several indicators, or several domains, depending on the nature of the concurrence that is being realized. In the example of Fig. 4, the indicator was the line V_i, determined by any pair of the points on it. V_i could have been equally well replaced by a quadratic curve (determined by any three of its points) or a cubic (determined by any four of its points not lying on a quadratic curve, i.e., of rank four), etc. This, in fact, is the implementation of shared secret schemes originally proposed by Shamir [53]. In this paper V_i and V_d will usually be restricted to be linear subspaces of some higher-dimensional containing space, S. In this case if $\dim(V_i) = k - 1$ and $\ell = k$, so that all of the private points are needed to span V_i, a k-out-of-k unanimous consent scheme results.

We will only consider a special case of the second type of scheme, namely, unanimous consent or k-out-of-k shared control schemes, which we will find useful later in a protocol to make it possible for a group of mutually distrustful participants—who don't

trust anyone else either—to establish a shared secret or shared control scheme that they must (logically) trust. Given k, the scheme is implemented in the k-dimensional space $\mathbf{S} = PG(k, q)$. The private pieces of information are k randomly chosen hyperplanes, that is, $(k-1)$-dimensional subspaces of $\mathbf{S}$, which almost certainly (with increasing q) intersect in only a single point p. If necessary, a particular choice for the k hyperplanes could be tested to verify that their intersection does not contain a line, but this is probably unnecessary. This is the natural generalization of the construction in Fig. 4 with only a pair of lines in the plane, that is, $\ell = 2$, and of Fig. 5 with a triple of planes in 3-space, that is, $\ell = 3$, etc. Although shared secret schemes of this type can be made for any ℓ, $k \leq \ell \leq (q^{k-1})/(q-1)$, we will not make use of them for values of $\ell > k$.

For much of this chapter we will be concerned only with shared secret schemes of the first type where $\mathbf{S}$ is a projective space $PG(n, q)$ over some finite field $GF(q)$. However, our examples will generally be constructed in affine spaces $AG(n, q)$, because of the closer analogy to the more familiar Euclidean spaces. Occasionally this will require a note of explanation to deal with special cases, but this should cause no confusion.

Our constructions make essential use of a simple result in projective geometry known as the rank formula:

$$r(U) + r(V) = r(U \cap V) + r(U \cup V) \tag{10}$$

true for all subspaces U and V of the containing space $\mathbf{S} = PG(n, q)$. $r(x)$ denotes the rank of the subspace x. Note that $r(x) = \dim(x) + 1$, and that the empty subspace has rank 0, and consequently dimension -1. It is easy to see that Eq. (10) does not hold in affine spaces. In $AG(3, q)$ there are pairs of parallel lines, that is, pairs of lines that do not intersect, but whose union is only a plane: $r(U \cap V) = 0$ and $r(U \cup V) = 3$ so that

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

From the standpoint of geometric intuition, Eq. (10) is more accessible if rank is replaced by dimension:

$$\dim(U) + \dim(V) = \dim(U \cap V) + \dim(U \cup V) \tag{11}$$

Constructions where $V_i \cup V_d = \mathbf{S}$ and $V_i \cap V_d = p$, p a point, make it possible to construct perfect (k, ℓ)-threshold scheme for any choice of k and ℓ. For a given q the dimension and hence the cardinality of the domain space V_d is chosen so that the probability of any collusion being able to (randomly) guess the secret point p, even though V_d is publicly known, is small enough to satisfy the security requirements. Let $\dim(V_d) = m$. The containing space, $\mathbf{S}$, is then chosen to be n-dimensional, where $n = m + k - 1$ and V_i is a $k-1$ dimensional subspace chosen so that $\dim(V_i \cap V_d) = 0$, etc. The private pieces of information in such a construction are points in V_i distinct from p, such that every subset of k of them span V_i and no subspace spanned by fewer than k of them lies on p. This guarantees that every subset of k (or more) participants can recover V_i and hence p, but that every point in V_d will remain an equally likely candidate to any collusion involving fewer than k participants. We will discuss this construction again in Section 5, which is devoted to implementing shared control schemes: It is described here so that we will have a ready example of (k, ℓ)-threshold schemes to use in Sections 3 and 4. The following four examples illustrate this result.

A pair of distinct lines, λ_1 and λ_2, in a plane define (span) the plane by their union and a point, p, by their intersection (Fig. 7):

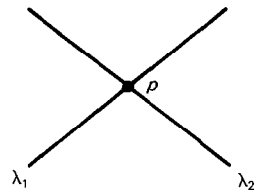

Figure 7

Similarly a plane, π, and a line, λ, not in the plane in a 3-space define (span) the 3-space by their union and a point, p, by their intersection (Fig. 8):

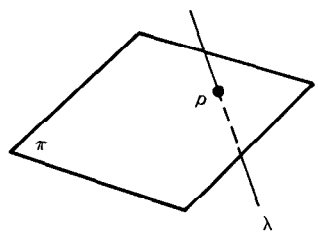

Figure 8

In the plane or in a three-dimensional space, these are the only possible configurations of this type. The following pair of examples in a four-dimensional space, **S**, indicates the usefulness of Eq. (11). In a four-dimensional space any pair of planes π_1, and π_2, that do not lie in a common three-dimensional subspace, intersect in a single point. Since they do not lie in a common three-dimensional subspace the dim $(U \cup V) = 4$, so that we have

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

hence, $U \cap V = p$, p a point. We will represent this four-dimensional construction with Fig. 9:

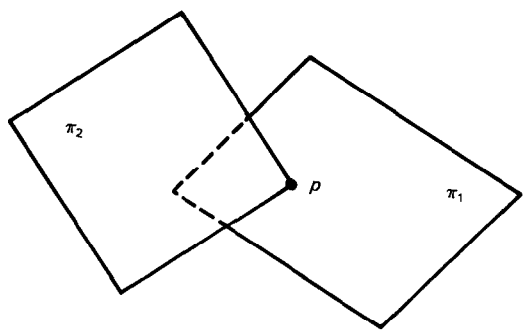

Figure 9

Similarly, a three-dimensional subspace, ω, and a line, λ, which span **S** must have a point, p, in common as well (Fig. 10):

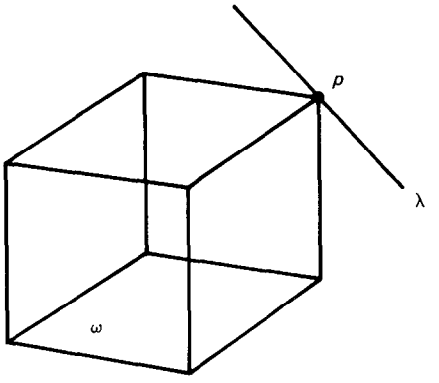

Figure 10

In Section 4 we will continue this discussion of geometric results essential to shared secret schemes, however, for the moment the four configurations in Figs. 7–10 suffice to illustrate everything we wish to show about threshold schemes. We have already seen how a 2-out-of-ℓ scheme can be implemented using the configuration in Fig. 7 by choosing ℓ points on one of the lines (none of which are the point p) as the private pieces of information, etc. This is the only type of shared control scheme that can be implemented using this configuration. The situation is different, however, for the configuration shown in Fig. 8. A 2-out-of-ℓ scheme is the only possibility if the private pieces of information are taken to be points on the line λ, however, several quite different concurrence schemes are possible if the private pieces of information are points in the plane π. For example, if the points are chosen so that they are distinct from p and no three of them are collinear and no pair of them are collinear with p, then any subset of three of the points will define π and hence p, but no subset of one or two of them will provide any information about p at all. This is one implementation for a perfect 3-out-of-ℓ shared secret scheme. p in this case is an unknown point on the (assumed publicly known) line λ. An identical set of remarks holds for the configuration in Fig. 9 except that in this case the secret can be any point in a (assumed publicly known) plane instead of on a line. The index point, p, since it must satisfy the linear constraints to lie in the plane V_d has an entropy of $H(p) = 2\log_2(q)$, that is, the same as that of a randomly chosen point in $GF(q) \times GF(q)$. The entropy-preserving transformations on p would therefore effectively map $p \in V_d$ onto $GF(q) \times GF(q)$. We will return to these configurations in much greater detail, however, these brief remarks should make clear the general nature of the constructions we will use for shared secret schemes.

3 CONSTRUCTING CONCURRENCE SCHEMES

In the application of shared control schemes, normally the first thing to be specified is the identification or description of the set of participants in the scheme and of those subsets (concurrences) of them who are authorized to initiate the controlled action. This could be as simple as requiring the concurrence of both participants where only two are

involved as is the case for opening and relocking of safety deposit boxes where both the box holder's key and the banking institution's key are required or in the U.S. policy of two-man control of the information used to control nuclear weapons where two pieces of information must be brought together to reconstitute the controlling information. Or, as we will see in a discussion of problems arising in connection with treaty-controlled actions, the schemes may be exceedingly complex with the participants having greatly different and noninterchangeable capabilities insofar as recovering the secret information is concerned.

Given a set of participants, a *concurrence scheme* (or *access structure* [3,19,20]) is a specification of those subsets of participants who are to be able to initiate the controlled action. A *collusion* is defined to be any set of participants or of participants and outsiders (to the shared control scheme) that doesn't include at least one set from the concurrence scheme. No collusion should be able to initiate the controlled action. We remind the reader that if the probability of being able to initiate the controlled action is the same for every collusion of participants as it is for an outsider, the scheme is perfect. A scheme is said to be *monotone* if every set of participants that includes at least one subset from the concurrence scheme is also able to initiate the controlled action. While this is certainly a natural condition to impose on shared control schemes, that is, if A and B together can initiate an action, then A, B, and C together should also be able to do so, nonmonotone schemes have been considered [8]. We will only consider monotone schemes here, however.

In the most extreme case, a concurrence scheme could take the form of a tabulation of all of the subsets of participants who are supposed to be able to recover the secret or initiate the controlled action. For a monotone scheme there is no reason to list sets that properly contain one or more sets also in the concurrence scheme; in other words, ABC would not need to be listed if any one of the sets AB or AC or BC is in the scheme. In many cases (covering most applications encountered thus far), there are much more succinct descriptions of the concurrence scheme than a listing of the subsets in it. For example, unanimous consent schemes where all of the participants must concur for the secret to be reconstituted or the controlled action initiated are described simply as unanimous consent or k-out-of-k shared control schemes; the second terminology has the advantage of identifying the number of participants involved. The identification of a concurrence scheme as a k-out-of-ℓ shared control or (k, ℓ) threshold scheme is much more compact than the tabulation of the $\binom{\ell}{k}$ k-sets that make up a (set containment) basis for the scheme. All of the concurrence schemes we will be concerned with here have such succinct descriptions as an artifact of their origin in applications where the specification of the desired control is similarly succinct.

The simplest class of schemes (to describe) are k-out-of-k unanimous consent schemes for which two implementations have already been given: in one of which k linearly independent points are chosen to span a $(k-1)$-dimensional subspace, V_i, of $\mathbf{S}$ that points to the secret point p in another subspace V_d, $\dim(\mathbf{S}) \geq k$, and in the other, k independent hyperplanes are chosen in $\mathbf{S}$, $\dim(\mathbf{S}) = k$, whose intersection is the point p. There is another way to construct a unanimous consent scheme which is already widely used, and which is a useful building block in the construction of other, more complex, concurrence schemes.

To be consistent with the discussion of the other two examples of implementations of unanimous consent schemes, we will also examine a 2-out-of-2 concurrence scheme in this case as well. If it is desired that a specific two persons (controllers) must concur

for a vault to be opened (or a weapon enabled or a missile fired) then each of these controllers could—during the initialization of the locking mechanism in the vault door—enter a randomly chosen k-digit number whose value is kept secret by the controller who chose it. The mod 10 sum of these two private and secret k-digit numbers would be the secret k-digit combination needed to open the vault. The subsequent entry of any pair of k-digit numbers whose mod 10 sum is equal to the secret combination determined by the two controllers would open the vault door. Clearly the probability that an outsider or either of the two insiders (controllers) alone being able to open the vault on the first try would be 10^{-k}. In this control scheme, two controllers are involved, and both must (in probability) concur in order for the controlled event to be initiated. This approach has in fact been used by the United States to protect critical shared command and control information.

In general, in a space whose cardinality is suitable for the concealment of the secret, that is, in which the probability of selecting a randomly chosen secret (point) in a subsequent random drawing provides an acceptable level of security for the controlled action, each participant chooses a random point as his contribution to the unanimous consent control scheme. If q is large enough to satisfy the security requirements there is no reason to not choose S to be one-dimensional (Fig. 11):

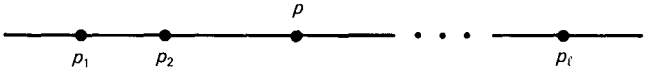

Figure 11

During the initialization of the mechanism that implements the shared control, each of the participants secretly enters the point he has selected and the sum (field, modular, exclusive-or, etc.) of all of the points becomes the jointly defined secret value. Since this procedure is an obvious generalization of Vernam encryption, the secret is unconditionally secure from discovery (or recovery) by any concurrence of fewer than all of the participants so long as the sum operation is an entropy-preserving mapping. To see that this is true, assume the worst-case scenario in which all of the participants but one conspire in an attempt to initiate the controlled action without the cooperation of the single missing participant. They can calculate the point that is the sum of all of their contributions, however, every point in the space is equally likely to be the secret point depending on the point chosen by the missing participant, since the sum operation is entropy-preserving. In other words, even in this worst-case scenario, the best that the would-be cheaters can do is to "guess" at the value of the secret using a uniform probability distribution on the points in the space. Clearly, this is the best that can be achieved with any shared control scheme.

There has been considerable interest in characterizing various classes of concurrence schemes. Brickell [18] and Brickell and Davenport [19] have discussed the characterization of ideal and strongly ideal secret sharing schemes while Benaloh and Leichter [3] have shown that there exist monotone secret sharing schemes that are not ideal. We shall restrict attention here, however, to only two general types of concurrence schemes—multilevel and multipart (or compartmented) schemes—and to arbitrary combinations of these types, since these are adequate to satisfy all applications known to the author.

A multilevel scheme is characterized by the participants having differing capabilities to initiate the controlled action. We described one such scheme earlier wherein either two vice-presidents or three senior tellers at a bank could authenticate an EFT. If there is no requirement that a vice-president also be able to act in the stead of a senior teller, it would be trivial to set up a shared control scheme with this concurrence. Separate and independent 2-out-of-ℓ_2 and 3-out-of-ℓ_3 shared control schemes could be set up for the two classes of participants, such that both schemes revealed the same point p. Assuming that q is sufficiently large that the guessing probability of $1/(q+1)$ for choosing p in a random drawing of the points on a line is adequately secure, V_d can be taken to be a line. The dimension of the two indicator varieties must be $k-1$, that is, 1 for Class I and 2 for Class II. Schematically, this may be shown as in Fig. 12:

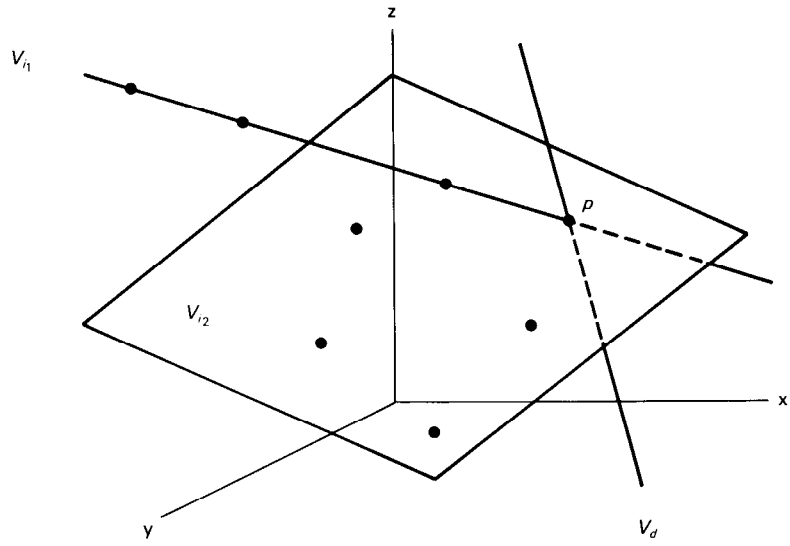

Figure 12

where the line V_{i_1} does not lie in the plane V_{i_2}, but both V_{i_1} and V_{i_2} intersect the line V_d in the point p. The private pieces of information for the Class I participants consist of points on V_{i_1} distinct from p, while the private pieces of information for the Class II participants consist of points in the plane V_{i_2}, also distinct from p, but chosen so that no three of them are collinear and no pair of them are collinear with p.

In Section 5, which is devoted to the implementation of shared control schemes, we will discuss the more difficult questions concerning how many participants there can be in each of the classes; that is, the bounds on ℓ_2 and ℓ_3, but for the moment we are only concerned with the essential notions underlying multilevel shared control schemes. In the implementation of Fig. 12, the classes are clearly independent, that is, no combination of a point on V_{i_1} and a pair of points in V_{i_2} can define a plane that intersects V_d at p since this would require that the pair of points in V_{i_2} be collinear with p, contrary to the way the private points were chosen.

If, however, we want it to be possible for any member of Class I in cooperation with any pair of members from Class II to be able to recover p, which is the concur-

rence scheme described earlier, then V_{i_1} must be a line in the plane V_{i_2} and the choice of the private points for the Class II participants must satisfy two additional constraints. No Class II point can be on the line V_{i_1} and no pair of them can be collinear with a point assigned as a private piece of information to any Class I participant. This latter requirement is essential; otherwise the private pieces of information held by this set of three participants (one from Class I and two from Class II) would only span a line skew to V_d and hence would be unable to recover p. We shall see below that all of these constraints are easy to satisfy. Schematically, the construction for this two-level shared control scheme in which the members of the more capable class can also act as members of the less capable class is of the form (Fig. 13):

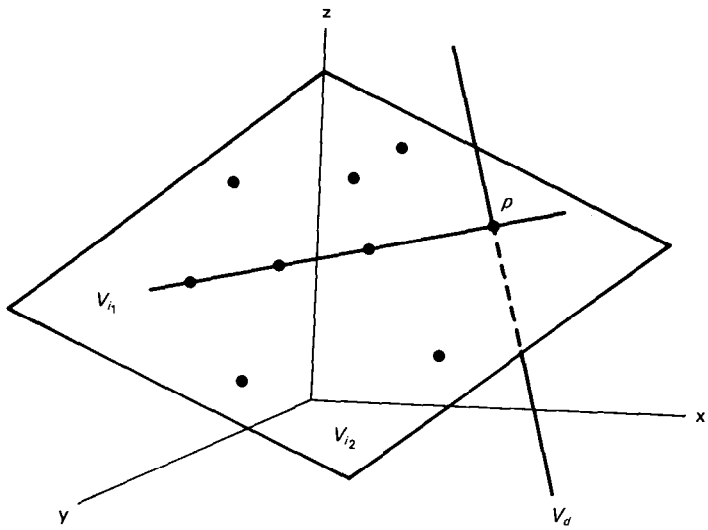

Figure 13

where the private points in the indicators V_{i_1} and V_{i_2} have been chosen subject to the constraints just described. Although we won't discuss the details of how to construct other multilevel schemes at this time, these two examples should at least make plausible the assertion that the general construction for k-out-of-ℓ shared control schemes can be extended in an obvious—and feasible—way to realize general multilevel schemes.

In all of the shared control schemes described thus far, the participants, even though they may have differing capabilities to recover the secret, are "on the same team." It is easy to conceive of situations, however, in which it is desirable that some action require a preselected level of concurrence by two or more parties for the action to be executed where the interests of the different parties may be quite divergent. For example, a treaty might require that two individuals out of a Russian control team and two individuals out of a U.S. team agree that a treaty-controlled action is to be taken before it could be initiated. What is different about such a compartmented scheme from either the simple k-out-of-ℓ schemes or the multilevel 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 prescribed 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.

Again we will use the smallest example that illustrates the essential notions to a multipart or compartmented scheme: Two parties (nations) are involved and they must both concur in order for a controlled action to be initiated. If each nation has only a single controller who is empowered to act as their representative, in other words, to act solely on his own to contribute his nation's input to the shared control scheme, a simple 2-out-of-2 unanimous consent scheme will suffice. We have already shown three ways to realize such unanimous consent schemes in the configurations in Figs. 4, 5, and 11: using only two private points on the line V_i in the first case, two private lines lying on the point p in the second, and two private points in S whose "sum" is p in the third. The fact that there are two nations or two parties involved is immaterial. There are two participants and both must concur for the controlled action to be initiated. If, however, each nation has not a controller but a control team, and in view of the importance of the controlled action each nation requires some degree of concurrence among its control team members before their national input to the control scheme can be made, the situation is quite different. Assume that each control team, of say, the United States and the USSR, consists of four members and the concurrence of at least two of them is required before their national commitment can be made. In this case a collusion of as many as five participants, say all four of the U.S. controllers in collusion with one of the USSR controllers, should be unable to initiate the treaty-controlled action while a concurrence of only four participants consisting of any two of the U.S. controllers with any two of the USSR controllers should be able to do so. We will exhibit four quite different implementations of shared control schemes that realize this two-part concurrence scheme.

It is easier to see how to adapt the constructions in Figs. 5 and 11 to realize the desired concurrence than it is to see how to adapt the construction shown in Fig. 4. In the Blakley-type scheme in Fig. 5, instead of each national controller being given—as his private piece of information—the line on p that is his nation's input to the shared control scheme, each member of a national control team would be given a point on the national line as his private piece of information (Fig. 14).

If one of the participants (in either team) were given the point p as his private piece of information, he would have no way of knowing that this was the shared (se-

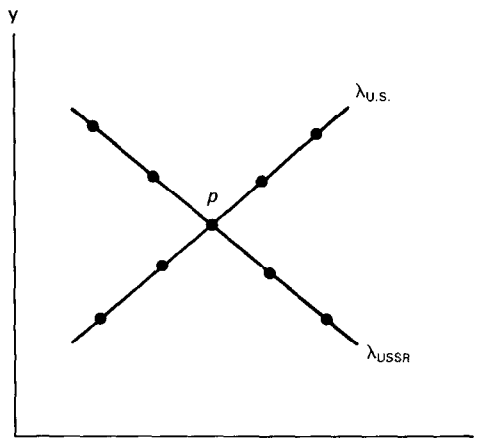

Figure 14

cret) point. This would be equally true for all collusions that did not include a pair of members from the other team. However, a collusion involving the participant who knows p and a pair of members of the other team could infer that p is the secret, since p lies on the line their points determine and hence must be the intersection of the two national lines. Therefore, only q of the $q + 1$ points on each line are available for use as private pieces of information: $L = q$ for each control team in this case. The resulting scheme is ideal, but not perfect, since any collusion including a pair of members from one of the national teams can restrict p to be a point on a line that they can unilaterally determine. It does have the desired property, though, that no collusion can recover the secret p, with a security equal to the probability of guessing an element in $GF(q)$, that is, $1/q$. We remind the reader that in this implementation, there are no indicator and domain varieties even though the secret point is defined by the intersection of a pair of subspaces.

The 2-out-of-2 unanimous consent scheme based on the construction shown in Fig. 11 is easy to adapt to an implementation of the desired two-party concurrence scheme. The line, λ, on which the 2-out-of-2 scheme is implemented, is embedded in the plane and the national lines, $\lambda_{\text{U.S.}}$ and λ_{USSR}, on which the 2-out-of-4 shared national control schemes are implemented, are used to indicate the two input points $p_{\text{U.S.}}$ and p_{USSR} on λ and hence to define p (Fig. 15). It should be pointed out that although p is an arbitrary point on the line λ, that λ is not a domain variety, V_d, in the sense we have defined V_d above, since the private pieces of information are not used to span an indicator variety that points to p.

Neither of the points $p_{\text{U.S.}}$ and p_{USSR} can be used as one of the private pieces of information. If both were used, then the two individuals who were assigned the points $p_{\text{U.S.}}$ and p_{USSR} could recover p without needing the concurrence of any of the other participants. If only one of the points, say $p_{\text{U.S.}}$ was assigned, then this member of the U.S. team in cooperation with any two members of the USSR control team could recover p, in violation of the concurrence requirements. Therefore, only q points on each of the national lines are available for use as the private piece of information (in $PG(2, q)$. This scheme is perfect—unlike the scheme in Fig. 14—since every point on the line λ is an equally likely candidate to be p to either an outsider or to any collusion of insiders, and realizable in a two-dimensional space: $\mathbf{S} = PG(2, q)$ or $\mathbf{S} = AG(2, q)$.

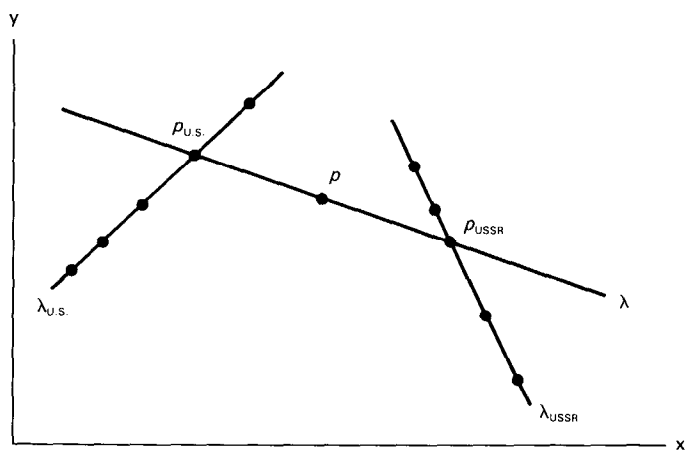

Figure 15

If the Shamir type of shared secret scheme is modified to realize the concurrence desired in this case, there are (at least) two possible constructions. With no loss of generality, we restrict the domain, V_d, to be a line in both constructions so as to keep the security the same in all of the constructions. A 2-out-of-ℓ scheme, $\ell > 2$, can only define a line as the shared subspace, hence the only thing that the national control teams can do (which others cannot) is to reconstruct the shared national lines $\lambda_{\text{U.S.}}$ and λ_{USSR}. One can either use these two lines (linear subspaces) as indicators to point to a pair of points in some other linear space which then determines a line in that space that can be used to point to the secret point p, or else take the linear subspace spanned by the two lines directly as an indicator, V_i, to point to p.

The first approach is intuitively the easier and also the one that lends itself most readily to generalization. The construction in Fig. 4 shows one way to implement a Shamir-type 2-out-of-2 unanimous consent scheme in a plane. We must somehow cause the two lines determined by the U.S. and the USSR control teams to in turn define a line, V_i, that indicates the point p in V_d. This must be done in such a way that all of the concurrence and security requirements are satisfied at the same time. One way to do this would be to make **S** be three-dimensional and to embed the plane, π, in which V_i and V_d occur in **S** (Fig. 16):

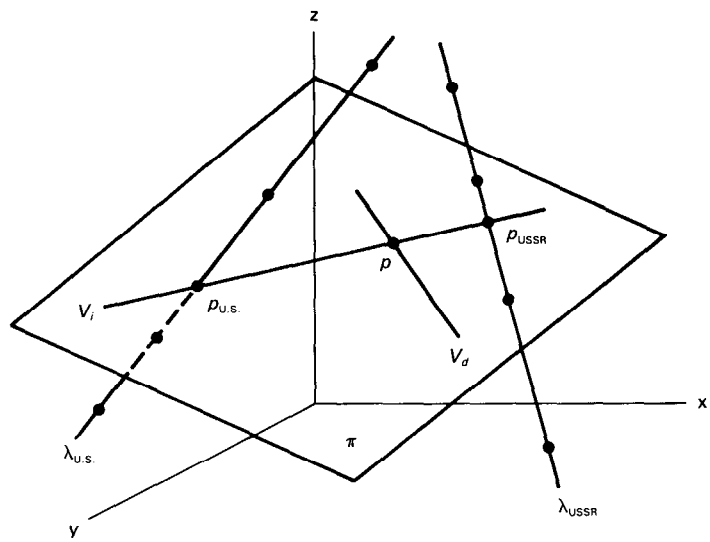

Figure 16

The private pieces of information in this case are points on the national lines, $\lambda_{\text{U.S.}}$ and λ_{USSR}, neither of which is in the plane π. The points, $p_{\text{U.S.}}$ and p_{USSR}, at which the national lines intersect π define the indicator V_i, and hence its intersection with V_d, in the point p. Any pair of points from the same control team define the corresponding line and hence the point at which this line intersects π; $p_{\text{U.S.}}$ or p_{USSR}. Neither of the points $p_{\text{U.S.}}$ or p_{USSR} in π can be used as one of the private points since a participant given such a point and knowing π would not require the concurrence of any other member of his control team to be able to make his nation's contribution to the

overall concurrence scheme. Therefore, as in the previous construction, q out of the $q + 1$ points on each of the national lines can be used as private pieces of information. Clearly, this scheme realizes the desired concurrence and security objectives with a security equal to the probability of guessing an element in $GF(q)$, that is, $1/q$. This scheme is perfect, since no collusion has any better chance of determining p than does an outsider—but not ideal.

Another way to implement the desired concurrence in this case would be to take **S** to be a four-dimensional space, and to let V_i and V_d be three-dimensional and one-dimensional subspaces of **S**, respectively, chosen so that; $\dim(V_i \cup V_d) = 4$ and $\dim(V_i \cap V_d) = 0$, that is, so that V_i and V_d intersect only in a point, p. Now if $\lambda_{\text{U.S.}}$ and λ_{USSR} are any pair of skew lines in V_i neither of which lies on p, we have the geometric basis for constructing a concurrence scheme with the desired properties (Fig. 17):

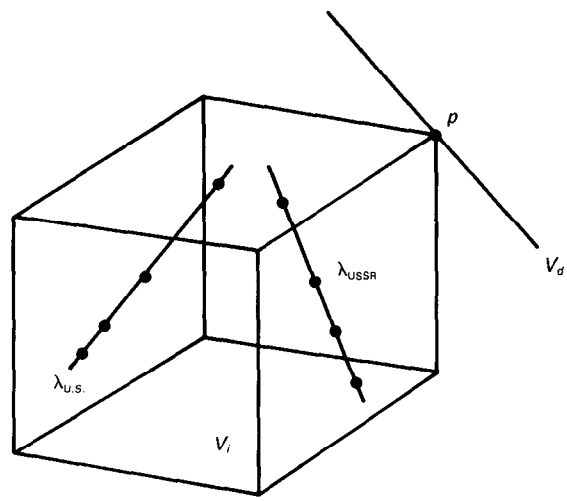

Figure 17

The private pieces of information are points on the two national lines $\lambda_{\text{U.S.}}$ and λ_{USSR}, chosen to satisfy a condition which we will describe momentarily. Clearly by the rank or dimension formula, the pair of skew lines span the three-dimensional subspace V_i, so that any subset of participants that includes at least a pair of members from each national team will be able to reconstruct V_i from the points they jointly know, and hence to recover p. The more difficult problem is to choose the private points in such a way as to insure that no subset of participants not satisfying this concurrence condition can do so.

It is an easy to see result in enumerative geometry that given two skew lines, λ_1 and λ_2, in a three-dimensional space and any point, p, not on either of the lines, that there is a single line lying on p and on both of the skew lines. p and λ_1 define a plane, π_1. Similarly p and λ_2 define a plane π_2. These planes are distinct since λ_1 and λ_2 are skew, hence they intersect in a line, λ^* which—by construction—lies on p and intersects both λ_1 and λ_2, say in points p_1 and p_2, respectively. If both of these points were

used as private pieces of information, then since they determine the line λ^* that intersects V_d at p, the two participants who were assigned p_1 and p_2 (one from the U.S. team and one from the USSR team) would be able to recover the secret without anyone else's assistance. Therefore it is not possible to use both of these points as private pieces of information. We will now show that it is not possible to use either of them.

Assume that p_1 on $\lambda_{\text{U.S.}}$ has been issued as a private piece of information to a member of the U.S. control team. Consider what can be inferred by this participant in collusion with at least two members of the USSR control team. They can determine the line λ_{USSR} that is skew to the line V_d, which is publicly known. λ_{USSR} and V_d together span a three-dimensional subspace which must contain the line λ^* since it contains two points on it; p_2 and p. By the result cited above from enumerative geometry, p_1, which is a point in the 3-space defined by the pair of skew lines λ_{USSR} and V_d and on neither of the lines, lies on a unique line intersecting both of the lines λ_{USSR} and V_d. Where it intersects the line, λ_{USSR} is of no interest, however, it is known a priori that it intersects V_d at p. Therefore a collusion of the participant who knows p_1 as his private piece of information and any two members of the other control team could recover p. Consequently neither p_1 nor p_2 can be used as a private piece of information and we have the same situation as in the two previous constructions; q out of the $q + 1$ points on each of the national lines can be used as private pieces of information with a security equal to the probability of guessing an element in $GF(q)$, that is, $1/q$.

Although the problem of making systems be perfect, or ideal, or extrinsic, etc. is very important to applications, we will defer further discussion of these topics for the moment. Instead we want to call attention to the most important feature of the construction in Figs. 15–17. In a subspace of **S**, we have a simple 2-out-of-2 unanimous consent scheme. Such a scheme requires the input of two functionally related points, $p_{\text{U.S.}}$ and p_{USSR}, for the secret point, p, to be determined. Each of the national concurrence schemes is a 2-out-of-4 shared control scheme pointing to the corresponding input point for the 2-out-of-2 scheme. In other words, we have constructed a lattice, organized as a tree in this case, of shared control schemes (Fig. 18):

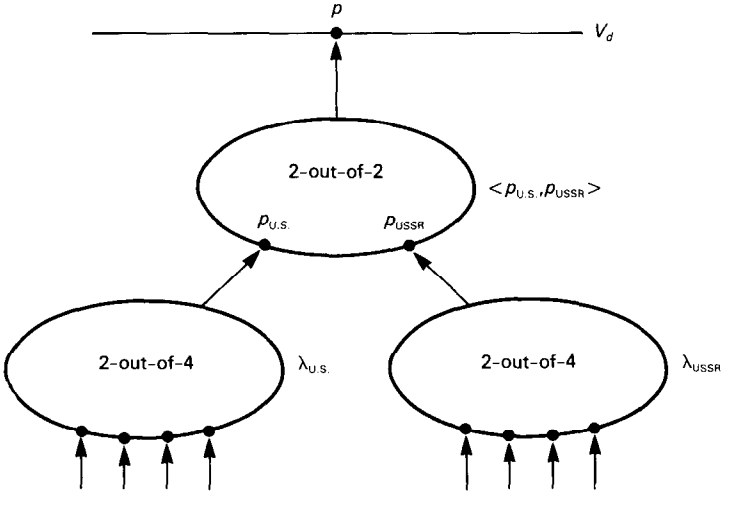

Figure 18

The notation $<p_{U.S.}, p_{USSR}>$ indicates the subspace of **S**—in this case a line—spanned by the objects (points) inside the brackets. Since the inputs to all of the shared control schemes we are considering are points in some space **S** or in subspaces of **S**, and the outputs are also points in **S**, we can construct shared control schemes of almost arbitrary complexity in this way. Let T be an arbitrary inverted tree, that is, with the edges all directed toward the root of the tree and let each node be a shared control scheme (k-out-of-k unanimous consent, k-out-of-ℓ threshold, k_i-out-of-ℓ_i multilevel—with or without interlevel capabilities—or multipart) with the input points for each node being defined by the shared control schemes on the nodes adjacent to it whose edges are directed into it and its output being an input point in the control scheme adjacent to it and above it in the inverted tree. The root control scheme defines the final indicator that points to the secret point, p, in V_d.

There are undoubtedly monotone shared control schemes not realizable in this way, although we know of no such example, however, all applications we have encountered can be satisfied with concurrence schemes that can be implemented as a tree of simple shared control schemes.

4 THE GEOMETRY OF SHARED SECRET SCHEMES

There are nongeometric constructions for shared secret schemes, most of which also have natural geometric interpretations. Asmuth and Bloom [2] generalized Vernam encryption to a modular cryptographic key sharing scheme. Several researchers have based secret sharing schemes on various properties of combinatorial designs: block designs [5,52], tactical configurations [33], perpendicular arrays [58,60], etc. Others have noted that the error-correcting property of error detecting and correcting codes can be used to recover the secret (codeword) from a perturbed version of it that can be formed by some subset of the participants, each of whom has partial information about the codeword [16, 47, 67]. Almost all of these constructions are examples of matroids, so that a few researchers have generalized shared secret schemes to their most abstract setting; matroids [18,19,61] or to general algebraic or logical systems [4,39,44,48,62,63]. In keeping with the development thus far in this chapter, we will only treat geometric schemes here, and, except for one application to make it possible for a group of participants who don't trust each other, nor any outside party, to set up a shared control scheme that they must (logically) trust, we will consider only the even more restricted class of extrinsic (ideal) systems in which the private pieces of information and the shared secret pieces of information are all points in a single space **S**.

The reader is already familiar with our preferred model for shared secret schemes: Any concurrence of the participants should possess a set of points that span a subspace (an algebraic variety in the more general setting) that intersects another (publicly known) subspace (algebraic variety) at the secret point p. What we plan to do in this section is to show how several plausible and/or real concurrence schemes can be realized. First, however, we state explicitly an important result that was only implicit in an earlier discussion. In the configuration shown in Fig. 7, **S** is two-dimensional and the two varieties, λ_1 and λ_2, are both lines, so that it is immaterial which of them is taken to be the subspace V_i and which to be V_d. In the configuration shown in Fig. 8 which we repeat here for the reader's convenience, **S** is three-dimensional and the subspaces are a plane, π, and a line, λ.

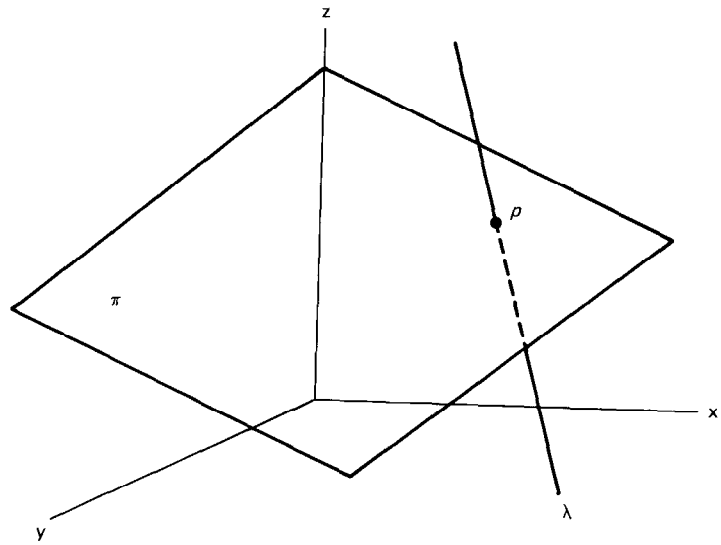

Figure 8 (repeated)

In this case, it makes a great deal of difference—from the standpoint of the concurrence schemes that can be realized—whether the indicator V_i is taken to be the line or the plane. Either choice is possible. This example illustrates an important duality principle: that for any geometric configuration consisting of two subspaces U and V of a projective space $\mathbf{S}$ in which $\dim(U \cup V) = \dim(\mathbf{S})$, $\dim(U \cap V) = 0$ and $\dim(U) \neq \dim(V)$, there exist families of dual shared secret schemes [55] depending on whether U or V is chosen to be the indicator V_i. If $V_i = \lambda$ in the present example, then the only concurrence possible would be a 2-out-of-ℓ shared control, $\ell \geq 2$. If $V_i = \pi$, however, at least four distinct concurrence schemes are possible.

If the private points (in π) are chosen to be different from p and such that no three of them are collinear and no pair lie on a line through p, then we have a perfect 3-out-of-ℓ scheme (Fig. 19). Although an explanation is probably unnecessary, the reason the points in π must satisfy these conditions is, first, if any pair of them is collinear with p, then, since the line they define must be in π, its intersection with V_d would have to be p—and the pair of participants knowing the scheme, but not π, would know this. Second, if any three of the points are collinear, then since the line they define does not intersect V_d, that is, is skew to V_d, these three participants would jointly be unable to define π and hence to recover p.

We remarked above that since the number of points on a line (in $PG(n, q)$) is $q + 1$, the order, q, of the ground field $GF(q)$ must be chosen sufficiently large that the probability of a random choice of points on V_d identifying p, namely, $1/(q + 1)$, will be small enough to satisfy the security requirements for the shared control scheme. There is another constraint, which is almost always trivially satisfied if the security constraint has been met: this is the number of participants that must be accommodated in the scheme. In the present case (the scheme shown in Fig. 19), the maximum number of points that can be chosen in a plane in $PG(3, q)$ such that no three of them are collinear is $q + 1$ if the characteristic of $GF(q)$ is odd, that is, if q is a power of an odd prime, and $q + 2$ if $q = 2^{\alpha}$ for some positive integer α.

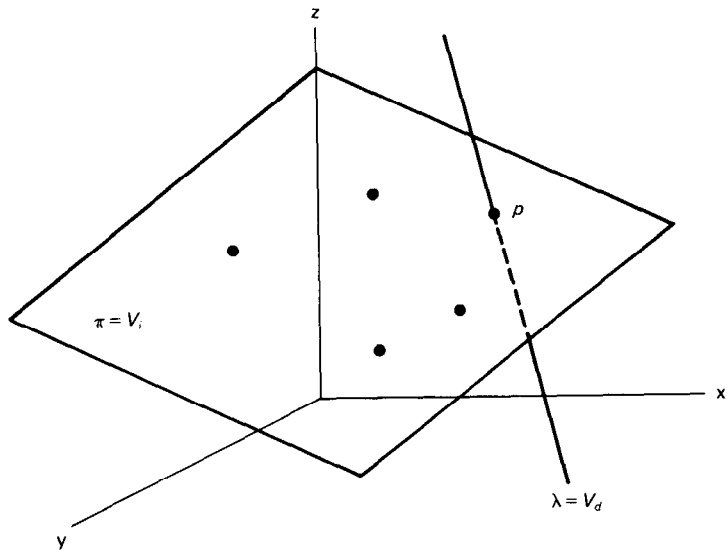

Figure 19

In the first case (q odd), such a maximal set of $q + 1$ points define a conic, Ω in the plane and the second case (q even), a conic, Ω, and its nucleus, η; that is, the point of common intersection of the $q + 1$ tangents to the conic. We will only be concerned with fields of odd characteristic. In this case, it is easy to determine a (sharp) upper bound, L, for the maximum number of participants such a 3-out-of-ℓ shared control scheme can accommodate. If p is an interior point of Ω, that is, if p does not lie on any tangent to Ω, then $L = (q + 1)/2$. This is obvious since any line on p and one point of Ω must also lie on another point of Ω; otherwise it would be a tangent to Ω, contradicting the assumption that p is an interior point. One and only one of this pair of points can be used as a private point. If p is an exterior point of Ω, then two tangents to Ω lie on p. The remaining $q - 1$ points can be paired by the same argument as before and one member of each pair used as a private point as well as the two points of tangency, or $(q + 3)/2$ points in all: $L = (q + 3)/2$. Because in applications, one normally wants high security which means large values of q and relatively few participants, it is unlikely that the order of the ground field will ever be dictated by the number of participants.

Continuing with the discussion of the concurrence schemes that can be realized using the configuration shown in Fig. 8, $\pi = V_i$ is also spanned by a line, λ^*, in π and any point, p', in π not on λ^*. Using this fact, we can realize a (plausible) two-part concurrence scheme. Assume that the United States wished to set up a shared control scheme with its 15 North American Treaty Organization (NATO) allies to control the first use of nuclear weapons in NATO such that at least two of the allies (other than the United States) had to concur before nuclear weapons could be used, but so that the United States retained an absolute veto power over this decision. This would mean that even if all fifteen of the European parties wanted to initiate the use of the nuclear weapons committed to NATO they would be unable to do so without U.S. concurrence, but it also means that the United States or the United States and any single ally would

be unable to do so by themselves. The two-part concurrence scheme shown in Fig. 20 realizes this type of shared control.

λ^* is a line in π that does not pass through the point p, that is, λ^* is skew to the line $\lambda = V_d$ in **S**. $p_{\text{U.S.}}$ is a point in the plane distinct from p and not on any line through p and one of the private points on λ^*. Clearly, any pair of the points on λ^* will determine it, but since it is skew to V_d every point on V_d is equally likely to be p to any collusion of non-U.S. participants. Since $p_{\text{U.S.}} \neq p$, and the ℓ lines defined by $p_{\text{U.S.}}$ with the ℓ private points on λ^* are all skew to $\lambda = V_d$, all collusions are equally unable to recover p as is an outsider; therefore the scheme is perfect. The point $p_{\text{U.S.}}$ and the line λ^* determine π and hence p, so that this configuration (Fig. 20) does realize the desired two-part shared control scheme. In this case, the line determined by the pair of points p and $p_{\text{U.S.}}$ intersects λ^* in a point that cannot be used as one of the private pieces of information. Therefore $L = q$ in this case, with $q + 1$ points in all in π being usable as private pieces of information. We mention this because we will encounter this same bound in other cases also.

In the previous section, we discussed a two-level shared control scheme, shown in Fig. 13, in which there were two classes of participants and the authorized concurrences were subsets that included either two members of Class I or three members of Class II or any member of Class I and two members of Class II. This scheme is also one of those that can be realized using the configuration shown in Fig. 8. We will not repeat the analysis of the security of the scheme here, but will briefly derive the bounds on the number(s) of participants such a scheme can support.

The first condition on the points chosen for the private pieces of information for the members of Class II is that no three of them can be collinear. As we have already remarked, for q odd this means that at most the $q + 1$ points on some conic, Ω, out of the $q^2 + q + 1$ points in π can be used (Fig. 21).

Since the line $\lambda = V_{i_1}$ must lie on p, and p cannot be used as a private piece of information, otherwise its holder, knowing V_d, would know that he had the secret, at

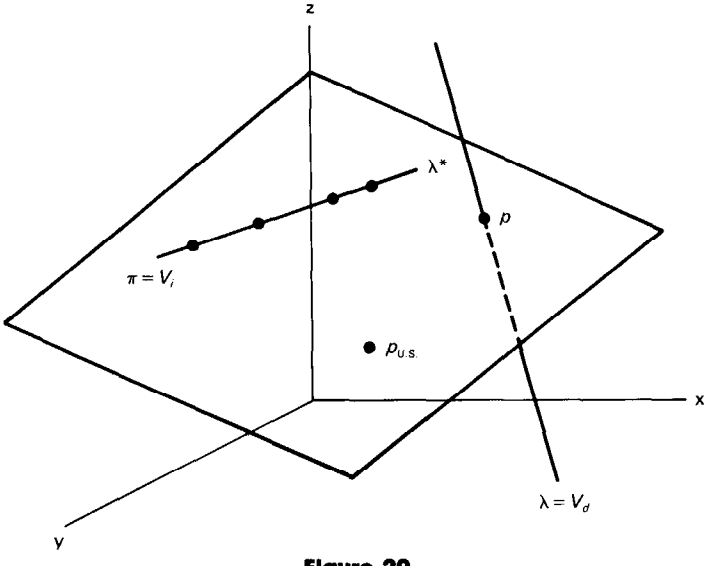

Figure 20

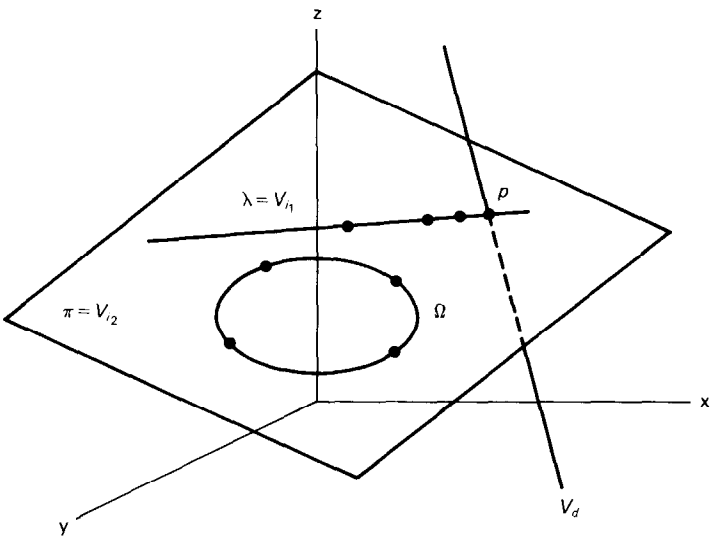

Figure 21

most q of the $q + 1$ points on λ can be used. The ℓ_3 Class III points on Ω determine $\binom{\ell_3}{2} = 0(\ell_3^2)$ distinct lines (secants of Ω) each of which intersects λ in a point that cannot be used as a private piece of information for the Class I participants—otherwise these three participants who form an authorized concurrence would only be able to determine a line skew to V_d which would leave all points on V_d equally likely candidates to be p, contrary to the concurrence requirements for the scheme. It is certainly conceivable that for $\ell_3 > \sqrt{q}$, all of the points on λ could be denied for use and Class I would be vacuous. In fact, if either λ or the set of ℓ_3 points on Ω are chosen randomly and ℓ_3 is only slightly larger than $\sqrt{q}$, this will almost certainly be the case. The surprising result is that by choosing the ℓ_3 points properly, it is possible to accommodate as many as q participants even when $\ell_3 = (q + 1)/2$. It is inappropriate to a survey report such as this to go into the mathematical detail needed to fully appreciate this result. The interested reader is referred to the mathematical literature [53,R2] for these details. We will describe only one of the several results of this sort.

For q odd, given any conic, Ω, in the projective plane $\pi = PG(2, q)$, and an exterior line, λ, to Ω, that is, a line that has no point in common with Ω, then λ induces a partitioning of the $q + 1$ points on Ω into sets of k points each, for every k that divides $q + 1$, such that the $\binom{k}{2}$ secants to Ω that they determine intersect λ in only k points! For example, if $q = 23$, then an exterior line λ partitions the 24 points on Ω into six sets of 4 points, four sets of 6 points, three sets of 8 points, and two sets of 12 points so that for any one of these sets, the 6, 15, 28, or 66 secants they define will intersect λ in only, 4, 6, 8, or 12 points, respectively. If the ℓ_3 points for the Class II participants are chosen in this way, then the remaining 20, 18, 16, or 12 points on λ can all be used either as the secret or private pieces of information for the Class I participants. The bottom line for the result just cited is that q out of the $q^2 + q + 1$ points in the plane can be used as private pieces of information in those cases where ℓ_3 is chosen to be a divisor of $q + 1$. A similar result holds, with different geometric constraints, for

the divisors of $q - 1$ and of q. The latter is only meaningful when $q = p^{\alpha}$, where p is a prime and α is a positive integer greater than 1.

We will not discuss bounds on the number of participants for any of the other schemes, since it should be clear by now that for the values of q needed to satisfy security requirements, the number of participants that can be accommodated will probably be much larger than any application will ever need.

It is worth pointing out that there is another choice for the private pieces of information for a 2-out-of-ℓ shared control scheme which can be based on the configuration in Fig. 22. Any pair of distinct lines in π span the plane, so we could use any ℓ distinct lines—not on p—as the private pieces of information.

Since a plane is two-dimensional in either points or lines, that is, the same amount of information is needed to specify an arbitrary one of either type, the scheme in Fig. 22 is equivalent to the 2-out-of-ℓ scheme based on points on a line (in π) as was done in the scheme shown in Fig. 13. The only possible advantage is that the maximum number of participants, L, can be greater in this case. One of the points on the line defined by the pairs of private points in the scheme shown in Fig. 13 must be the secret point p, so $L = q$ in that case. On the other hand, the number of lines in a projective plane is $q^2 + q + 1$, while the number that lies on the point p is $q + 1$. Therefore there are q^2 lines in the plane that do not lie on p and $L = q^2$ in this case. As we have already remarked, though, q is dictated by security constraints that cause it to be so large that it is inconceivable that an application would ever require $L > q$. This case has been included only for completeness. We will not consider any other schemes in this section in which the private pieces of information are not points in **S**.

The preceding discussion should give some indication of the rich diversity of shared control schemes that can be implemented from even a small geometric configuration of two subspaces that span **S** and have only a single point in common.

The balance of this section will be devoted to a discussion of a bare minimum of geometric results needed to analyze or to appreciate the analysis of the security of

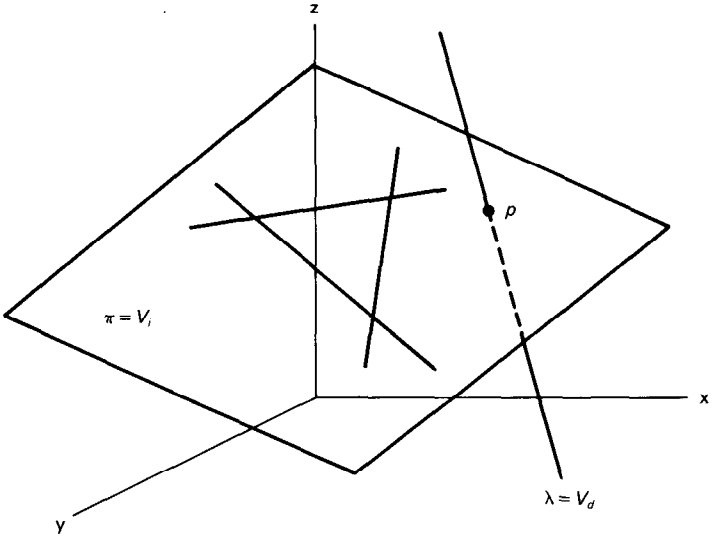

Figure 22

shared secret schemes. It can safely be skipped over if the reader is either already familiar with the geometry of finite spaces (affine and projective) or if he is only concerned with the essential notions of shared secret schemes and not with the details of their implementation.

In the discussion of the simple 2-out-of-ℓ shared secret scheme shown in Fig. 4 (which is repeated here), there were two (interrelated) points to the discussion of the scheme's security. The first had to do with showing that the scheme was perfect, that is, equally secure to all collusions—an outsider or a single insider in this case. The other had to do with the fact that the information content (in the information theoretic sense) of the private pieces of information did not all have to be communicated and protected as secret information. These two points must be considered for even the most general schemes as well.

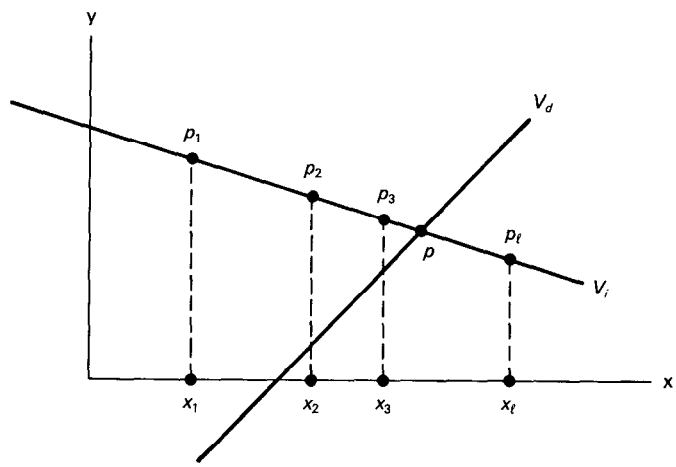

Figure 4

In the scheme in Fig. 4, it is public knowledge that the secret is a point p on V_d that has been chosen with a uniform distribution over all of the points in the subspace. Hence, the probability of an outsider successfully identifying p in a similar manner, when $\mathbf{S} = AG(2, q)$, is

$$P_d = \frac{1}{|V_d|} = \frac{1}{q} \tag{12}$$

Although the answer is obvious in this case, consider whether an outsider could improve his chances (of identifying p) by using his knowledge of the scheme itself and of the publicly exposed abscissas, x_j, of the participant's private pieces of information. He knows only that the indicator, V_i, is a line that is not parallel to the y-axis, but there are q such lines through every point on V_d and on each point on the vertical lines (x_j, y) for each of the x_j. Since these are all equally likely to be V_i, his odds of being able to guess V_i are only $1/q^2$, hence he would be better off to guess at p. The important point, however, is that the number of possible choices (for the line V_i) is the same for each possible choice of p. This would also have been true if the space had been $\mathbf{S} = PG(2, q)$, and in general for any space $\mathbf{S}$.

We have used the term "subspace" imprecisely—and will continue to do so—to indicate a geometric object in an affine space that is either a subspace or is isomorphic to a subspace. These objects are properly called *flats*, and only those flats that include the origin are actually subspaces. In $AG(2, q)$, for example, only the $q + 1$ lines that contain the point (0, 0) are subspaces. The other lines are 1-flats, the 1 indicating that they are one-dimensional objects, isomorphic to $AG(1, q)$, etc. We will use this precision of language only in the stating of the next few results.

The result we need is a well-known [R3,R4] formula that enumerates the number of k-dimensional subspaces or k-flats of $PG(n, q)$ or $AG(n, q)$ that contain a given t-dimensional subspace (flat), respectively. To this end, define the function $\varphi(n, k; q)$:

$$\varphi(n, k; q) = \begin{cases} 1 & k = 0 \\ \prod_{i=0}^{k-1} \left[\frac{q^n - q^i}{q^k - q^i}\right] & 1 \le k \le n \end{cases} \tag{13}$$

The number of distinct k-flats in $\mathbf{AG}(n, q)$ is

$$q^{n-k}\, \varphi(n, k; q) \tag{14}$$

and the number containing a given t-flat is

$$\varphi(n - t, k - t; q) \tag{15}$$

For example, Eq. (14) says that the total number of lines, 1-flats, in $AG(2, q)$ is

$$q^{2-1}\, \varphi(2, 1; q) = q^2 + q$$

and that the number of lines lying on a given point, Eq. (15), is

$$\varphi(2, 1; q) = q + 1$$

results we have already made use of.

Similarly, the number of k-dimensional subspaces in $PG(n, q)$ is

$$\varphi(n + 1, k + 1; q) \tag{16}$$

and the number containing a given t-dimensional subspace is

$$\varphi(n - t, k - t; q) \tag{17}$$

For example, Eq. (16) says that the number of one-dimensional subspaces in $PG(2, q)$ is

$$\varphi(3, 2; q) = q^2 + q + 1$$

and the number lying on a given point is

$$\varphi(2, 1; q) = q + 1$$

To see how these formulas can be used to calculate the security of a shared control scheme, let $\dim(V_i) = m$, $\dim(V_d) = s$ where as usual, $\dim(V_i \cup V_d) = \dim(\mathbf{S}) = n$ and $\dim(Vi \cap Vd) = 0$. Assume that a collusion of k' of the participants

pool their private pieces of information in an effort to improperly recover p. Together their points span a subspace T, where $\dim(T) = t \leq k' - 1$. $T \cap V_d = \phi$, since $T \subset V_i$ and $V_i \cap V_d = p$; otherwise the collusion would be able to identify p. Hence the subspace spanned by the k' points and an arbitrary point, p', in V_d, $<T \cup p'>$, will have dimension $t + 1$;

$$\dim < T \cup p' > = t + 1 \leq k'$$

Irrespective of whether we are in $AG(n, q)$ or $PG(n, q)$ Eqs. (15) and (17) state that the number of $(t + 1)$-dimensional subspaces (flats) lying on all $k' + 1$ of these points is uniformly $\varphi(n - t - 1, k - t - 1; q)$ for every choice of a point in V_d. In other words, every point in V_d is equally likely to be p given the private information available to any collusion, just as it is in the absence of any insider information. Neither can the collusion improve their chances by guessing at V_i among all of the m-dimensional subspaces that contain the k' known points and an assumed point, p', in V_d, since there are uniformly many of these for each choice of p' as well. Hence such schemes are perfect.

It is a little more difficult to show that it is only necessary for each participant to keep secret an amount of information equal to the information content of the secret itself. We have already shown that in a perfect shared secret scheme, which is the only type being considered here, at least this much secret information must be contained in each private piece of information. Given a shared secret scheme of this type, it may be the case that the subspaces V_i and V_d are not full rank with respect to the natural coordinate system. This possibility was why, in the scheme shown in Fig. 4, we excluded the $q + 1$ lines parallel to the y-axis, in $AG(2, q)$, from being used as the indicator V_i, since if V_i were chosen to be one of these lines and the abscissas, x_j, publicly exposed, then even an outsider would be able to determine p.

This geometric argument is easy to see, but the essential difficulty is that the functional expression for V_i in this case is singular with respect to the x parameter; that is, given x_j one cannot solve for y_j. Since $V_i \cup V_d = \mathbf{S}$—the two subspaces span $\mathbf{S}$—and $\dim(V_i) + \dim(V_d) = m + s = n = \dim(\mathbf{S})$ there is a rigid transformation, τ (consisting of rotations and translations) that maps p into the origin and has rank n, that is, any m of the coordinates of the points in V_i can be used to compute the other s coordinates, or any s of the coordinates of a point in V_d can be used to compute the other m.

If the initial subspaces V_i and V_d do not satisfy this condition, we will choose a transformation τ so that τV_i and τV_d do, after which an arbitrary (but fixed) set of s of the coordinate values in the private pieces of information must be kept secret while the other m can be publicly exposed. The integrity of the exposed coordinates must be insured since if an opponent could modify these (without being detected) he could deny an authorized concurrence the ability to initiate the controlled action by causing them to reconstruct an incorrect value for p. The geometric construction for shared secret schemes described here is both perfect and ideal, the latter implying the first as was pointed out above.

The significance of minimizing the amount of information that must be kept secret is that in real-world applications, this information must often either be committed to memory, or else be recoverable from a private cipher (by the participant) using a mnemonically reconstructed one-time key. In either case, there is a great premium on minimizing the amount of information that the participant must memorize.

5 SETTING UP SHARED SECRET SCHEMES

The discussion thus far has been solely concerned with how, and whether, a shared secret scheme can be designed to realize the desired concurrence and security specifications. The tacit assumption has been that when it came to setting up the scheme that there would be some third party, which could be either an individual or a device, that is unconditionally trusted by all the participants in the scheme. This trusted party would first choose the secret (piece of information) and then construct and distribute in secret to each of the participants the private pieces of information that are to be their shares in the shared secret or control scheme. These private pieces of information would be constructed as described at such length in this chapter to realize the desired concurrence scheme. Given the existence and assistance of such an unconditionally trusted third party, there is no conceptual difficulty in realizing any of the shared control schemes described here.

For many applications, however, such an autocratic scheme is not possible since there is no one who is trusted by all of the participants, and in the extreme case, no one who is trusted by anyone else. It is worth noting that in commercial and/or internation(al) applications, this situation is more nearly the norm than the exception. In the absence of a trusted party or authority, no one can be trusted to know the secret and hence, until now, it has appeared to be impossible to construct and distribute the private pieces of information needed to realize a shared control scheme.

The problem of setting up shared secret schemes in the absence of a trusted third party has been ignored by researchers in this area with the single exception of a paper by Meadows [48]. Meadows's paper discusses this problem and examines at even greater length the twin questions of how new participants can be enrolled in an already existing shared control scheme and of how previously enrolled participants can be cut out. To accomplish this, Meadows uses a construction that she calls a rigid linear threshold scheme which makes it possible for a predetermined number of the existing participants to delegate their capability to a new member—essentially to vote him into membership. Meadows's constructions do not appear to be related to the approach to be presented here, especially so since her primary proposal depends on a secure (unconditionally trustworthy) black box to replace the services of an unconditionally trustworthy key distribution center. Meadows attributes the question of whether a shared secret scheme can be set up without the assistance of a trusted key distribution center to Chaum. Chaum posed the question in a talk given in the Rump Session of Crypto'84 that was not published in the Proceedings for that meeting. The important point, however, is that Meadows's work appears to be the only prior published reference to the problem of how a shared control scheme can be set up without the assistance of a trusted key (share) distribution center.

The single exception to what has just been stated is that a way has been known (and used) for several years to insure unanimous consent before a controlled action can be initiated. These are schemes of the sort discussed in connection with the construction shown in Fig. 11 in which each participant secretly chooses a point—randomly and with a uniform probability distribution—from the same space, S, in which the secret point p occurs, and the "sum" of these private points is defined to be p. This implementation of shared control is in fact used by the United States for the control of sensitive command and control information. For anything other than a unanimous consent scheme, however, there must be some sort of functional dependence enforced between

the participants' private pieces of information reflecting the structure of the authorized concurrences—even though the participants don't trust each other so that cooperation can't be assumed. Until now, the only way a functional dependence could be enforced between uncooperative and distrusting parties was with the assistance of a third party who had to be unconditionally trusted by all of the participants to set up the shared control scheme.

The essential notion to a protocol devised by Ingemarsson and Simmons [38] to make it possible for parties that don't trust each other—or anyone else either—to set up a shared control scheme that they must (logically) trust is that the secret (piece of information) will be jointly determined in a unanimous concurrence scheme from inputs chosen and made privately by each of the participants. Each of these inputs is to be equally influential in determining the value of the secret and is itself to be kept secret by its contributor. Shared control schemes of this sort in which each participant has an equal influence on the determination of the secret (i.e., the information equivalent of the democratic principal of "one man, one vote") will be referred to as *democratic schemes*, as contrasted with *autocratic schemes* which presuppose the availability of an unconditionally trusted third party.

Once the secret has been determined, each participant may, if he wishes, devise private shared control schemes by means of which he can distribute among the other participants private pieces of information that would make it possible for some groupings of them to reconstruct his contribution to the determination of the secret. Since he is acting to protect his own interests, he can insure by means of the shared control schemes that he devises that only concurrences of participants whom he would be willing to trust to act in his stead will be able to reconstruct his contribution to its determination. This is sufficient to guarantee to each participant that his private contribution will be accessible only to concurrences that either include him as a member or else which are acceptable to him. Since each participant acts similarly, the net result is that by using this protocol, parties that do not trust each other can jointly set up a shared control scheme that they do trust.

The general protocol for a group of mutually distrustful participants to use to set up a shared control scheme that they must logically trust, without the assistance of any outside party, is therefore:

1. The participants first set up a democratic unanimous consent scheme; that is, one in which they each contribute equally to the determination of the secret point, p, and hence in which all of their private inputs (contributions) must be made available for the secret to be reconstructed. This step doesn't require that anyone trust anyone else.

2. After the unanimous consent scheme is in place, any of the participants who trust some concurrence(s), that is, subsets of the other participants, to faithfully represent their interests can then create private shared secret schemes to distribute information about the private (and secret) contribution they made to the determination of p. Thereafter those concurrences can act in their stead—and more importantly, no other collections of participants can do so. In setting up these private shared secret schemes each participant is acting as his own "trusted authority" to protect his own interests, so that he need trust no one else insofar as the delegation of the capability to act in his stead is concerned. In this way, each participant can guarantee that only concurrences that either include him as a member or else that include a subset of the other participants whom he trusts to represent his interests will be able to initiate the controlled

action or to recover the shared secret. But this is precisely the risk a participant would have had to accept if there had been an unconditionally trusted central authority to set up the shared control scheme in the first place.

The net result is that democratic shared control schemes of arbitrary complexity (of control) can be established that accurately reflect the placement of trust (or lack of it) by the participants in each other. In other words, every shared control scheme that would be acceptable to the participants and which could be set up by a mutually trusted authority (in Meadows's terminology, a trusted KDC), can also be set up as a democratic scheme by the participants themselves without anyone having to accept a greater risk of their interests being abused than they would have had to accept for a trusted authority to set up the scheme instead.

Given this insight into the nature of democratic shared controls schemes, a question of primary importance is how the initial unanimous consent scheme can be set up. Ingemarsson and Simmons [38] found that of all of the ways to implement unanimous consent schemes, there were apparently only two—inequivalent—ways to set up a democratic unanimous consent scheme.

Either way, of course, can serve as the starting point for setting up more complex schemes using the protocol described above. The first is simply a generalization of the example given earlier.

1. In a space whose cardinality is adequate for the concealment of the secret, that is, in which the probability of selecting a randomly chosen secret (point) in a subsequent random drawing provides an acceptable level of security for the controlled action, each participant chooses a random point as his contribution to the unanimous consent control scheme. During the initialization of the mechanism that implements the shared control, each of the participants secretly enters the point he has selected and the sum (field, modular, exclusive-or, etc.) of all of the points becomes the jointly defined secret point, p.

2. In a k-dimensional finite space where k is the total number of participants in the scheme and the cardinality of the space is chosen such that a hyperplane provides an adequate concealment for the secret point, each participant randomly chooses a hyperplane as his private contribution to the determination of the secret (point). The intersection of these k hyperplanes is then used to define the secret point, p. The important point is that k hyperplanes almost certainly (with q) intersect in only a single point, so that the protocol described here will almost certainly define a unique value for the secret in a democratic shared control scheme. In the event that they do not, this would be detected during the initialization phase of setting up the shared control scheme and the participants would have to make another (random) choice of their inputs (hyperplanes).

It might at first appear that these two protocols for setting up unanimous consent schemes are in some sense simply two versions of a single scheme; especially so in view of the geometric duality between points and hyperplanes when these objects are the private choices of inputs in the two protocols. It is easy, however, to show that this cannot be the case.

In the first scheme, the uncertainty about the secret is the same for an outsider as it is for every combination of fewer than all of the participants: namely, it is equally likely to be any point in the containing space. Furthermore, there is no relationship between the dimension of the space in which the secret is concealed and the number of

participants in the shared control scheme. The only requirement is that the number of points in the space be large enough that the probability of choosing the secret (one) at random will be sufficiently small. In other words, a k-out-of-k scheme could be implemented in a one-dimensional space as well as any other, even if the dimension of the containing space is greater than k.

On the other hand, in the second unanimous consent scheme the dimension of the space must equal the total number of participants, k. Otherwise the intersection of the k randomly and independently chosen hyperplanes will almost certainly over- or underdetermine a point; that is, the hyperplanes will either not have a common point of intersection or else they will intersect in a subspace of higher dimension. More importantly, however, outsiders and all proper subsets of the insiders will be faced with substantial differences in uncertainty about the secret. An outsider knows only that p is some point in $PG(k, q)$, where all points are equally likely, that is, an uncertainty of $O(q^{-k})$. Any one of the participants, however, knows that p must be a point in the hyperplane he chose, that is, a point in an $(k-1)$-dimensional subspace that is an uncertainty about p of only $O(q^{-(k-1)})$. Similarly, any pair of participants together could reduce the uncertainty about p to being a point in the $(k-2)$-dimensional subspace that is the intersection of the two hyperplanes they chose, etc.

There are other, geometric, arguments to show the inequivalence of these two protocols for setting up unanimous consent schemes in the absence of trust, but none so easy to see as this information-based argument.

The smallest example that fully illustrates the protocol would be a 2-out-of-3 threshold scheme: For instance, a scheme in which any two out of three vice-presidents at a bank can open the vault door but in which no one of them alone can do so. The constructions for 2-out-of-ℓ shared control schemes shown in Figs. 4 and 5 require the assistance of a trusted third party to set them up initially, and as we have already mentioned, don't seem to be realizable without such outside assistance. We will now show how the three vice-presidents can set up such a scheme using either of the two unanimous consent democratic schemes described earlier. In either case, the combination (secret) can be thought of as a point in some suitable space.

For the first unanimous consent scheme the secret can be taken to be any point, p, on a line. Each of the three participants secretly and randomly chooses a point, p_i, on λ. p is defined to be the field sum of the three points:

$$p = \sum_{i=1}^{3} p_i \tag{18}$$

Clearly Σ satisfies the definition of an entropy-preserving sum, since as any single summand, p_i, ranges over all $q+1$ possible values, with the other two points remaining fixed, so does the sum p.

The inescapable conclusion that follows from the acceptability of a 2-out-of-3 threshold scheme is that each participant is willing to trust the other two participants jointly to only initiate the controlled action (i.e., to open the vault door in the present example) when they should. By the same token, the need for a 2-out-of-3 concurrence presupposes a lack of confidence in what a single individual might do. Consequently each participant (in this example) must logically be willing to share his private input to the secret between the other two participants in such a way that they can jointly reconstruct his contribution, but are individually not only unable to do so but are totally

uncertain of it. To do this, each participant constructs a private 2-out-of-2 scheme of the sort described earlier, that is, he randomly chooses a pair of points whose sum is his contribution to the democratic shared secret scheme, and gives (in secret) each of the other participants a different one of these points. A convenient way to represent this implementation of the protocol is:

	1	2	3
1	p_1	p_{21}	p_{31}
2	p_{12}	p_2	p_{32}
3	p_{13}	p_{23}	p_3

where the three points in column i are all chosen by participant i—subject to the condition that $p_i = \sum_{j \neq i} p_{ij}$. The three entries in row j are known to participant j: the entry on the diagonal because he chose it and the off-diagonal entries because they are the private pieces of information (points) given to him by the other participants. Clearly, any two participants have between them all the information needed to compute $p = \Sigma\, p_i$, while any one of them is totally uncertain as to the value of p. Although we have described the protocol starting with the establishment of the democratic unanimous consent scheme, the scheme would probably be implemented in reverse order. Participant i would choose at random the two points p_{ij}, $j \neq i$, and then calculate his input, p_i, to the unanimous consent scheme $p_i = \sum_{j \neq i} p_{ij}$, etc.

To set up the other type of unanimous consent scheme each participant chooses at random a plane in a projective 3-space $PG(3, q)$. As was noted above, since there are three participants, the second type of scheme is only possible in a three-dimensional space. With virtual certainty (with increasing size of q), the three randomly and independently chosen planes intersect in only a single point. This point, p, is the jointly determined secret (combination) $p = \cap_{i=1}^{3} \pi_i$. This protocol defines a 3-out-of-3 unanimous concurrence scheme (such as was shown in Fig. 3) in the case $\ell = 3$, because the three vice-presidents acting together can cause the secret to be reconstructed within the vault door mechanism at any time by reentering their private pieces of information (planes).

As before, each participant also sets up a private 2-out-of-2 shared secret scheme to distribute information about the plane he chose to the other participants, constructed so that they can jointly reconstruct his plane, but individually cannot do so. One way he could do this is by choosing any pair of distinct lines lying in his plane and giving a different one of these lines to each of the other participants. Since the lines are distinct, taken together they span the plane. Hence any two vice-presidents have between them the capability to reconstruct all three planes and thus redefine p.

The private pieces of information for each participant will be the plane he chose and the two lines given to him by the other vice-presidents. Since the pair of lines are shares in a perfect 2-out-of-2 scheme defining his secret plane, each vice-president is assured that a successful concurrence must either include him as a participant or else include both of the other vice-presidents. A convenient way to represent this implementation of the protocol is

	1	2	3
1	π_1	λ_{21}	λ_{31}
2	λ_{12}	π_2	λ_{32}
3	λ_{13}	λ_{23}	π_3

where the lines (off-diagonal) entries in column i are chosen by participant i—subject to the condition that they span the plane π_i, $\pi_i = \cap_{j \neq i} \lambda_{ij}$. The three entries in row j are known to participant j: The entry on the diagonal because it is the plane he chose and the off-diagonal entries because they are the private pieces of information (lines) given to him by the other participants.

This small example illustrates the bare bones of the protocol from the standpoint of making sure that no participant can increase his capability beyond what is acceptable to the other participants.

The bottom line is that the protocol described in this section permits democratic shared secret schemes, which must logically be trusted, to be set up by mutually distrustful parties without outside assistance. In addition, no participant is required to accept a greater risk of the secret information being misused than what he would have had to be willing to accept if there had existed a trusted authority to set up the scheme instead. Clearly, this is the most that can be hoped for from any protocol. It should also be pointed out that if other protocols for setting up democratic unanimous consent schemes (to the two described here) are discovered, the protocol can be adapted to use them as well.

6 KEY DISTRIBUTION VIA SHARED SECRET SCHEMES

Shared secret schemes were originally devised by Shamir and Blakley as a means of key management in cryptosystems—to insure against authorized users being denied use of the system due to a loss of the key and to prevent unauthorized persons from being able to use the system as a result of the key being compromised. In this section we will explore shared secret schemes as a means of handling key distribution for some applications.

The primary motivation for developing the multilevel schemes discussed above was to provide protection from what is known as a decapitation attack. Although this terminology is suggestive, it may not be self-explanatory. If there is information that is held by a higher level of command that must be communicated to lower levels in order for some action to be initiated—such as arming warheads, launching missiles, etc.—an adversary may attempt to prevent the action from being initiated by destroying the higher level in a surprise attack before the information can be disseminated to the lower levels of command. This is called a *decapitation attack*. There is another aspect to decapitation attacks in that if the higher levels of command are destroyed, the lower levels either may not know what to do or else be ineffectual in their response. We are not concerned with these consequences to a decapitation attack, however, but only with the situation in which the lower levels of command are rendered incapable of carrying out an action, that they are otherwise able to do, because one or more pieces of information needed to initiate the action were prevented from reaching them by the attack on the superior command.

Multilevel shared control schemes were devised specifically to solve this problem in situations in which the lower level of authority (and hence responsibility) at a lower level of command could be satisfactorily compensated for by requiring an increased level of concurrence for the action to be initiated. There are certainly many situations in which this is the case and for which the multilevel schemes discussed earlier provide a means of solution. There are actions, however, in which either the law doesn't permit a

delegation of authority (and hence capability), irrespective of the concurrence that might be required for it to be exercised, or else in which the party(ies) holding the capability are not willing to delegate the capability under normal circumstances. The crucial words in this description are "under normal circumstances," implying that there are circumstances that would either permit such a delegation to be made or in which such a delegation would be acceptable. The problem, from the standpoint of the shared secret or shared control scheme, is the same in either case.

Consider a missile battery at which there are a dozen officers. The consequences of a missile being launched without proper authority would be so great that in normal times (peacetime or in lower levels of alert) the capability to initiate such an action is to be held at a higher level of command, perhaps by the president; in other words, the policy is that even if all of the officers at the battery believe that a missile should be launched, they should not be able to do so without requesting authorization from the superior commander (and more importantly, could not do so without being given the launch enable codes).

In the absence of a shared control scheme, the only way that the superior commander could protect against a decapitation attack on his headquarters (and him) would be to preemptively enable the missiles as a part of going to an advanced state of alert. But these are precisely the circumstances in which there is the greatest concern that something might go wrong and a missile could be launched when it shouldn't have been. Requiring the concurrence of k of the battery officers, say two of them, for a launch is a way of increasing confidence in the proper execution of the plan of battle. What is needed is a scheme in which, under normal circumstances, only the superior commander has the capability to enable a missile launch, but that would allow him, when intelligence inputs or other early warnings indicate, to delegate a k-out-of-12 shared control of the launch to the battery to prevent a decapitation attack from succeeding. The problem is: How does he establish the k-out-of-12 shared control scheme at the time the battery goes to an advanced state of alert? If no advance arrangements have been made, the 12 pieces of private information would have to be communicated to the battery officers in a secure and authenticated manner, at a time (advanced stage of alert) when communications are apt to be both congested and disrupted. Even if the information could be communicated to the battery at that time, the risk of human error in dealing with unfamiliar codes of a size at the limits of mnemonic aids to memorization would be high.

Ideally, it should be possible to distribute the private pieces of information in advance of a need to use the shared control scheme, but with the constraint that in normal circumstances even if all of the participants were to violate their trust and pool their private pieces of information they would still have no better chance of recovering the secret than an outsider would have of simply guessing it. In such a scheme, at the time the battery is put in an advanced state of alert, a single piece of information (one share in the terminology introduced earlier) would need to be communicated by the superior commander to activate the prepositioned k-out-of-12 shared control scheme so that any k of the officers would thereafter be able to launch the missiles.

The important point to this discussion is that almost all of the information needed to implement the shared control (the private pieces of information) could be communicated in advance of the need during a time of low tension and reliable communications. Since there is no special urgency during this setup phase, the communication could even be handled by courier or by having the officers in the subordinate command come

to headquarters to be given their private pieces of information. At a time when the battery is going to a state of advanced alert, that is, a period of high tension when communications are at a premium, only a single share (the minimum amount) of information needs to be communicated to activate the scheme.

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

Another equally important problem has to do with how the battery can stand down from an advanced state of alert, where standing down means reverting to the kind of control that existed prior to the alert. For this to be possible, the scheme must provide both a capability for the superior commander to activate the shared control scheme (delegate authority) and to deactivate it, that is, to rescind his delegation of authority, if the circumstances change so that an advanced state of alert is no longer warranted. If the system is to truly revert to the same type and quality of control after a recall that it had prior to the alert without changing the private pieces of information involved in the shared control scheme, then both the activating information that is to be sent by the superior commander and the enabling code that the missile will respond to must change with each delegation of authority, irrespective of whether the delegated capability was exercised or not.

Although it is inappropriate to the purpose of this discussion to say much about the practical problems of implementing shared control schemes that change with time or use, it is perhaps worthwhile remarking that there are two ways (at least) to achieve this. The simplest scheme would be for the enable codes to change automatically as a function of time, say once each day. Another approach would be for the mechanism in the missile controller that carries out the calculation of the secret information from the private pieces of information to have a stored list of enabling values, only one of which would be operational at a time. In a scheme of this type, the activating piece of information that is sent by the superior commander would have to correspond to the current value of the secret if the shared control is to be operable. If a recall is received (from the superior command), its entry would advance the store to the next stored value for the secret and output a piece of information that could only be obtained by executing this protocol. This would return the missile to a condition wherein only the superior commander could enable it for a launch or delegate its release if the battery was later put in an advanced state of alert again. The old value of the secret information would become invalid so that stale values of the activating information would not be operable. The unique output that could only be obtained by properly carrying out the recall protocol could be returned to the superior command to verify that the control system had been returned to its prealert status.

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

1. It should be possible to preposition all of the private information needed for the shared control scheme subject to the condition that even if all of the participants were to violate the trust of their position and collaborate with each other, they would have no better chance of recovering the secret information than an outsider has of guessing it; that is, the scheme should be perfect.
2. It should be possible to activate the shared control scheme once it is in place by communicating a single share of information, and for many applications, it should also be possible to reveal different secrets (using the same prepositioned private pieces of information) by communicating different activating shares of information.

To achieve multilevel and multipart shared control schemes, we modified the indicator, V_i, in some cases to multiple independent indicators (Fig. 12) or to multiple geometrically nested indicators (Fig. 13) or to multiple functionally related indicators (Figs. 16 and 17), etc. To achieve the shared control capabilities just described, we will find it necessary to modify the domain variety V_d; in some cases by withholding it, that is, keeping it secret from the participants and the outsiders alike, until the controlled action is to be authorized, and in others by having multiple domains—either independent or functionally related, etc. Roughly speaking, extended concurrence is achieved by refinements of V_i while extended control is achieved by refinements of V_d.

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

In the example of a 2-out-of-ℓ shared secret scheme shown in Fig. 4, both V_i and V_d were lines in the plane $\mathbf{S}$. Since a plane is two-dimensional in both points and lines, two shares of information, that is, the identification of two elements from $GF(q)$, are required to specify either one in the affine plane $AG(2, q)$. In other words, the same amount of information would have to be communicated to identify p as a general point in $\mathbf{S}$ as would have to be communicated to identify V_d. This might seem to indicate that two shares of information would need to be communicated to activate the scheme, instead of the information theoretic minimum of a single share. However, given V_i (or else V_d) p is no longer an arbitrary point in the plane but rather an unknown point on a line, whose specification on that line requires only one share of information. Similarly, given that p is constrained to be a point on V_i, V_d no longer need be free to be an arbitrary one of the q^2 lines in the plane not parallel to the y-axis, but can instead be restricted to be one out of a set of q lines in which one line lies on each point of V_d.

One easy way to do this would be to preposition an x-coordinate, x_d, different from the point at which V_i intersects the x-axis at the time the scheme is set up. Later, when the scheme is to be activated, the y-intercept of the line V_d through the points x_d and p is all that would need to be communicated to permit V_d to be determined. Thereafter, any two of the participants could recover V_i using their private points, and hence recover the secret p.

If we construct a 3-out-of-ℓ scheme based on the configuration shown in Fig. 9 in which S is four-dimensional and V_d is a plane, the problem is even more difficult to deal with since 4-space is six-dimensional in planes while the secret is only two-dimensional in information content. While a similar, but more complex, resolution is possible in which four out of the six needed shares of information would be prepositioned along with the private pieces of information required to set up the shared secret scheme, and the remaining two shares communicated at the time the scheme is to be activated, there is a more efficient (and general) way to implement such schemes. Table 1, tabulating the dimension of the space of m-flats in an n-dimensional space, suggests how difficult this problem can become. If V_i and V_d were both three-dimensional, which only permits a 4-out-of-ℓ shared control, the space of 3-flats is already twelve-dimensional, meaning that 12 shares of information are required to identify V_d.

TABLE 1. DIMENSION OF THE SPACE OF m-FLATS IN AN n-DIMENSIONAL SPACE

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

In Section 2, which was devoted to the general model(s) for shared secret schemes, we discussed at length the differences between the two approaches to realizing such schemes. In one of these approaches a concurrence of points (the private pieces of information) spanned an indicator, V_i, that pointed out the secret point p, while in the other approach, p was defined by the intersection of a concurrence of geometric objects, each of which contained p. Our principal observation was that while the first scheme was inherently perfect, the other could never be if p was regarded as the secret itself, but that both schemes provided the same level of security in a very natural sense for the shared secret information. In particular, if the information revealed by the second type of scheme was viewed as a cryptographic key, the equivalence in security between the two types of schemes was easy to see.

The problem, arising in our earlier identification of V_i with a cryptographic key, is that the revelation of the secret was equated with the identification of the point p at which the secret is determined. p is not itself the secret, but rather some entropy-

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

To illustrate this implementation, consider again the simple 2-out-of-ℓ scheme shown in Fig. 4 when used with the DES encryption algorithm. The plane in this case would be $AG(2, 2^{56})$. Each private piece of information would consist of 112 bits, 56 of which would have to kept secret by the participant, and 56 of which need only be protected against substitution, alteration, or destruction or loss. V_d, or rather two shares of information (112 bits) adequate to determine V_d, would be prepositioned at the time the scheme was set up. After this has been done, any two of the participants, using their private pieces of information, could determine V_i and hence recover p which in this case would be a 2-tuple in $AG(2, 2^{56})$.

There is no reason to not use the simplest entropy-preserving function available; namely, let the secret DES key be the y-coordinate of p, since by the constraints on the construction in this example all 2^{56} possible values are equally likely. Thus an authorized concurrence could recover the DES key at any time after the scheme was set up, however, they could not recover the secret(s) until such time as a cipher was communicated.

On the other hand, the secret (plaintext) would be secure even if the cipher had been communicated unless an authorized concurrence of the participants cooperated to recover the key and decrypt the cipher. In those applications where it was either tolerable or acceptable that a proper concurrence be able to recover the secret at any time after the scheme was fielded, the cipher(s) could be prepositioned along with the private pieces of information. In situations such as those considered in this section, the cipher(s) could be withheld until it is desired that the scheme be enabled, at which time the minimum of only one share of information would have to be communicated for each secret that is to be revealed.

7 CONCLUSIONS

When it comes to implementing a shared control scheme for a specific application, there is an important point that needs to be considered, but which hasn't been; namely, when there is more than one implementation for a shared secret scheme satisfying the concurrence and security requirements, which is the best. To illustrate: Assume that the management of a bank that has a dozen vice-presidents wishes to set up a shared control scheme so that a (arbitrary) pair of the vice-presidents must concur for the vault to be

opened, and that the security of this scheme is to be such that the likelihood of any collusion (an outsider or a vice-president or an outsider and a vice-president) being able to open the vault will be 1 in a million or less on their first attempt. Since $2^{20} = 1{,}048{,}576 > 10^6$, such a scheme could be implemented using the 2-out-of-ℓ scheme shown in Fig. 4 with $q = 2^{20}$. p is an arbitrary point on the line V_d, so the security is just the probability, P_s, of guessing p

$$P_s = \frac{1}{|V_d|} = \frac{1}{q} < 10^{-6}$$

as desired. This also means that the vault lock would have to accept 2^{20} different combinations for this result to be true. We will assume therefore that the input mechanism for the vault accepts binary strings; that is, the vault door is opened by a 20-bit combination. The private pieces of information (points on V_i), on the other hand, require two shares or 40 bits for their specification. As we have made clear in earlier discussions, these 40 bits do not all need to be kept secret: 20 bits must be kept secret while it suffices for the participant to merely insure the integrity of the other 20.

In the scheme of Fig. 4, implemented in $AG(2, q)$, there are q points on each line, $q - 1$ of which could be used as private pieces of information, that is, the scheme could accommodate over a million vice-presidents when only a dozen are needed. This is a wasted capability, bought at the expense of increasing the amount of information (in the information-theoretic sense) in the private pieces of information. If instead, a 2-out-of-ℓ scheme were implemented using the configuration shown in Fig. 8 with V_i being the line λ and V_d being the plane π, then $q = 2^{10}$ would suffice, since $|V_d| = 2^{20}$, etc. as before. In this case, only 30 bits would be needed in the private pieces of information; of these 30 bits, 20 would still have to be kept secret, while only 10 would need to have their integrity assured. This is still an extravagant scheme though since over a thousand vice-presidents could still be accommodated. If, however, **S** is taken to be a six-dimensional space over $q = 2^4$ and V_d taken to be a five-dimensional subspace of **S**, then $|V_d| = 2^{20}$ as before, and V_i would be a line with only $q = 16$ points on it. In this case, the dozen vice-presidents could be accommodated (with three slots to spare) and the private pieces of information would consist of only 24 bits.

A more informative example is provided by the three two-part schemes shown in Figs. 15–17. The concurrence implemented in all three of these schemes requires that both of the national inputs be available in order for the controlled action to be initiated, where each national input is itself controlled by a 2-out-of-4 threshold scheme. The subspace, V_d, was chosen to be a one-dimensional subspace in each case. Hence, if the security requirement is that the likelihood of a collusion being able to identify p on the first try, is to be no better than 1 in a million, then $|V_d| = q > 10^6$. As in the previous example, this requirement could be satisfied by taking $q = 2^{20}$, etc. Since the space **S** in which the constructions are made is two-dimensional (Fig. 15), three-dimensional (Fig. 16), and four-dimensional (Fig. 17), respectively, this would mean that the private pieces of information would have to be 40-, 60-, and 80-bit binary numbers, only 20 bits of each of which would have to be kept secret and the integrity of the remaining bits insured. It is possible, however, to do much better than this. A 2-out-of-ℓ, $\ell > 2$, threshold scheme can only define a line in **S** irrespective of the dim(**S**). Since in each construction we showed that only $q - 1$ out of the q points on a national line (in $AG(n, q)$) could be used as private pieces of information, to accommodate four control

team members $q \geq 4$. $q = 2^2$ would therefore be one possibility. If we set $q = 2^2$, then $\dim(V_d)$ must be at least 10 to meet the security requirements.

The equivalent generalization of the configuration in Fig. 15 requires an eleven-dimensional space, **S**, in which V_d is a ten-dimensional subspace. The lines $\lambda_{\text{U.S.}}$ and λ_{USSR} are lines in **S** that do not lie in V_d but are not skew to it either and hence intersect V_d in single points, $p_{\text{U.S.}}$ and p_{USSR}. Just as in the two-dimensional construction these can be any pair of points in V_d, so that their sum p is also (equally likely to be) any point in V_d. The private pieces of information in this case are 22-bit binary numbers, all numbers being equally likely.

The generalization of the configuration shown in Fig. 16 is a little more difficult to visualize. As before, V_d is a ten-dimensional subspace in **S** and p is any point in V_d. The line V_i is an arbitrary line in **S** lying on p, but not in V_d. Let T be the subspace $<V_i, V_d>$ spanned by V_i and V_d. In other words, $\dim(T) = 11$. $p_{\text{U.S.}}$ and p_{USSR} are any pair of distinct points on V_i, not equal to p. $\lambda_{\text{U.S.}}$ and λ_{USSR} are a pair of lines lying on $p_{\text{U.S.}}$ and p_{USSR}, respectively, but not in the subspace T. $\lambda_{\text{U.S.}}$ and λ_{USSR} satisfy the condition that $\lambda_{\text{U.S.}} \subset <\lambda_{\text{USSR}}, T>$ and $\lambda_{\text{USSR}} \subset <\lambda_{\text{US}}, T>$. In other words, **S**, which is the space spanned by $\lambda_{\text{U.S.}}$, λ_{USSR}, and T is twelve-dimensional. This construction is both easy to do and uniform independent of the choices of lines, points, etc. The private pieces of information in this case would be 24-bit binary numbers—all numbers being equally likely, etc., as in the previous case.

Finally, the generalization of Fig. 17 requires that $\dim(\mathbf{S}) = 13$ with V_d being a ten-dimensional subspace and V_i a three-dimensional subspace, where $\dim(V_i \cup V_d) = 13$ and $\dim(V_i \cap V_d) = 0$. In this case, the private pieces of information would be 26-bit binary numbers—with the same conditions regarding secrecy and integrity as before.

The whole point in developing this second example has been to illustrate another criteria, other than the information content of the private pieces of information, for deciding which among several implementations of equivalent shared secret schemes is best. Assume that the application needed to accommodate more than two parties, but that the concurrence of (any) two was sufficient for the controlled event to be initiated. The first implementation (the generalization of the configuration in Fig. 15) cannot add even one more party, that is, it cannot even be extended to a 2-out-of-3 party concurrence, since the sum operation (used to define p) is restricted to a unanimous consent scheme.

On the other hand, in the second implementation (the generalization of the configuration in Fig. 16) $q - 1$ out of the q points on the line V_i could be used as national inputs, hence a total of three national parties could be accommodated in this case in a 2-out-of-3 party concurrence scheme. Obviously,each of the national points on V_i must be distinct, otherwise any two parties whose national lines defined the same point would be unable (together) to define V_i and hence to recover p, in contradiction of the concurrence requirements.

The analysis of the third implementation is a bit more difficult. Given that the ten-dimensional subspace, V_d, has been identified and a point p randomly chosen in it, the two national lines are chosen to be both skew to V_d and to each other, and hence they define a three-dimensional subspace V_i that intersects V_d only in the point p. To add another party to the concurrence scheme so that any two of the parties could identify p, the private pieces of information for the members of this party's control team would have to be points on a third line in V_i skew to V_d and to each of the lines $\lambda_{\text{U.S.}}$

and λ_{USSR}. The question of how many parties could be accommodated by such a scheme is thus equivalent to the geometric question: Given a point p in a three-dimensional affine space, T, what is the maximum number of pairwise skew lines that can be chosen in T such that no line lies on p? We first answer this question in $PG(3, q)$ and then use this result to answer the question in $AG(3, q)$. It is easy to see that there are at most q^2 such lines in $PG(3, q)$. The number of points in the space is

$$\varphi(3, 0; q) = \frac{q^4 - 1}{q - 1} = q^3 + q^2 + q + 1$$

Since the lines are pairwise skew, no point is on two of the lines. There are $q + 1$ points on each line, hence an upper bound for the number of pairwise skew lines is

$$\# \leq \frac{\varphi(3, 0; q)}{q + 1} = q^2 + 1 \tag{19}$$

If equality holds in Eq. (19), the lines partition the points of T, hence p must be on one of these lines and the other q^2 could be used as the national lines for different national parties. It is well known that such partitions (called spreads) of $PG(3, q)$ by lines do exist [R3, R4], hence the generalization of the configuration shown in Fig. 17 could accommodate as many as q^2 parties in $PG(3, q)$. Given a spread of $q^2 + 1$ lines in $PG(3, q)$, let π be an arbitrary plane. π contains $q^2 + q + 1$ points, each of which must be on one line of the spread, but there are only $q^2 + 1$ lines in the spread so that one line of the spread must be in π. π could not contain two lines of the spread since they could not then be skew lines. Therefore every plane in the space contains one line of the spread and intersects every other line in a distinct point. To answer the question for $AG(3, q)$, take an arbitrary spread in $PG(3, q)$ and delete the plane at infinity. This leaves q^2 skew lines, each of which has q points, that partition the points of the space. p lies on one of these lines. The remaining $q^2 - 1$ pairwise skew lines could all be used as national lines in a 2-out-of-ℓ multiparty shared control scheme; hence as many as 15 parties could be accommodated.

The point of this example has been that while the information content of the private pieces of information differed very little in this case, the number of parties that could be accommodated varied significantly; 2, $q - 1$, and $q^2 - 1$, respectively. If the capability to enroll new parties (even one additional party) is a significant consideration, this would rule out using the scheme that minimizes the information content of the private pieces of information.

The bottom line to this is that the concurrence scheme determines the dimension of V_i while the security requirement dictates the cardinality of V_d. There is in general a range of geometric implementations satisfying both of these conditions, with the final choice being determined by which scheme is optimal by some other measure; in the first example, by minimizing the information content of the private pieces of information and in the second by whether the desired number of parties could be accommodated by the scheme. Different applications will have differing criteria as to which implementation is "best." The point of these concluding remarks is that for a given set of concurrence and security requirements, there are in general many different implementations for shared control schemes that satisfy the requirements—if an implementation exists at all—and that the decision as to which of these is the best must come from other considerations.

References

[R1] *American National Standard, X9.17-1985*, "Financial institution key management (Wholesale)," American Bankers Association, Washington D.C. April 4, 1985.

[R2] W. Jackson, "On designs which admit specific automorphisms," Ph.D. Thesis, Mathematics Department, University of London, Royal Holloway and Bedford New College, 1989.

[R3] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, Oxford Mathematical Monographs, Oxford: Clarendon Press, 1979.

[R4] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford Mathematical Monographs, Oxford: Clarendon Press, 1985.

Bibliography (Shared Secret Schemes)*

[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. Security and Privacy*, Oakland, CA, April 26–28, 1982, pp. 156–169. Los Angeles: IEEE Computer Society Press, 1982.

[2] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 2, pp. 208–210, March 1983.

[3] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto '88*, S. Goldwasser, Ed., Santa Barbara, CA, Aug. 21–25, 1987, pp. 27–35. Berlin: Springer-Verlag, 1990.

[4] J. C. Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret secret," in *Lecture Notes in Computer Science 263; Advances in Cryptology: Proc. Crypto '86*, A. M. Odlyzko, Ed., Santa Barbara, CA, Aug. 11–15, 1986, pp. 251–260. Berlin: Springer-Verlag, 1987.

[5] L. Berardi, M. DeFonso, and F. Eugeni, "Threshold schemes based on criss-cross block designs," private communication available from G. J. Simmons.

[6] L. Berardi and F. Eugeni, "Geometric structures, cryptography and security systems requiring a quorum," *Proc. 1987 ATTI del Primo Simposio Nazionale su Stato e Prospettive della Ricerca Crittografica in Italia*, Rome, Italy, Oct. 30–31, 1987, pp. 127–133, 1987; in Italian, English translation available from G. J. Simmons.

[7] A. Beutelspacher, "Enciphered geometry: Some applications of geometry to cryptography," Proc. Combinatorics '86, in *Annals of Discrete Mathematics*, vol. 37, A. Barlotti, M. Marchi, and G. Tallini, Eds., pp. 59–68. Amsterdam: North-Holland, 1988.

[8] A. Beutelspacher, "How to say 'no'," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt '89*, J.-J. Quisquater and J. Vandewalle,

---

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

Eds., Houthalen, Belgium, April 10–13, 1989, pp. 491–496. Berlin: Springer-Verlag, 1990.

[9] A. Beutelspacher and K. Vedder, "Geometric structures as threshold schemes," 1986 IMA Conference on Cryptography and Coding, Cirencester, England, in *Cryptography and Coding*, H. J. Beker and F. C. Piper, Eds., Oxford: Clarendon Press, pp. 255–268, 1989.

[10] G. R. Blakley, "Safeguarding cryptographic keys," *Proc. AFIPS 1979 Natl. Computer Conf.*, New York, vol. 48, pp. 313–317, June 1979.

[11] 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. Los Angeles: IEEE Computer Society Press, 1980.

[12] G. R. Blakley and R. D. Dixon, "Smallest possible message expansion in threshold schemes," in *Lecture Notes in Computer Science 263; Advances in Cryptology: Proc. Crypto '86*, A. M. Odlyzko, Ed., Santa Barbara, CA, Aug. 11–15, 1986, pp. 266–274. Berlin: Springer-Verlag, 1987.

[13] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Lecture Notes in Computer Science 196; Advances in Cryptology: Proc. Crypto '84*, G. R. Blakley and D. Chaum, Eds., Santa Barbara, CA, Aug. 19–22, 1984, pp. 411–431. Berlin: Springer-Verlag, 1985.

[14] 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. Los Angeles: IEEE Computer Society Press, 1981.

[15] J. R. Bloom, "A note on superfast threshold schemes," preprint, Texas A & M University, Department of Mathematics, 1981.

[16] J. R. Bloom, "Threshold schemes and error correcting codes," in *Abstracts of Papers Presented to the American Mathematical Society*, vol. 2, 1981, p. 230.

[17] J. Bos, D. Chaum, and G. Purdy, "A voting scheme," presented at Crypto '88, Santa Barbara, CA, August 21–25, 1988. Presented at Rump Session but not published in the Proceedings of the conference (copies available from the authors).

[18] E. F. Brickell, "Some ideal secret sharing schemes," presented at 3rd Carbondale Combinatorics Conference, Oct. 31, 1988, Carbondale, IL; in *J. Combinatorial Math. and Combinatorial Computing*, vol. 6, pp. 105–113, Oct. 1989. Also in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt '89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10–23, 1989, pp. 468–475. Berlin: Springer-Verlag, 1990.

[19] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," in *Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto '89*, G. Brassard, Ed., Santa Barbara, CA, Aug. 20–24, 1989, pp. 278–285. Berlin: Springer-Verlag, 1990.

[20] E. F. Brickell and D. R. Stinson, "The detection of cheaters in threshold schemes," in *Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto '88*, S. Goldwasser, Ed., Santa Barbara, CA, Aug. 21–25, 1987, pp. 564–577. Berlin: Springer-Verlag, 1990.

[21] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," University of Nebraska, Department of Computer Science, Report Series no. 106, May 1990; *J. Cryptology* (in press).

[22] D. Chaum, "Computer systems established, maintained, and trusted by mutually suspicious groups," Memo. No. UCB/ERL/M79/10, University of California, Berkeley, Electronics Research Laboratory, 1979; also D. Chaum, Ph.D. dissertation in Computer Science, University of California, Berkeley, 1982.

[23] D. Chaum, "How to keep a secret alive: Extensible partial key, key safeguarding, and threshold systems," in *Lecture Notes in Computer Science 196; Advances in Cryptology: Proc. Crypto '84*, G. R. Blakley and D. Chaum, Eds., Santa Barbara, CA, Aug. 19–22, 1984, pp. 481–485. Berlin: Springer-Verlag, 1985.

[24] D. Chaum, C. Crepeau, and I. Damgård, "Multiparty unconditionally secure protocols," 4th SIAM Conf. Discrete Math., San Francisco, CA, June 13–16, 1988, abstract appearing in *SIAM Final Program Abstracts: Minisymposia*, no. M-28, p. A8, 1988.

[25] 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, pp. 383–395, Oct. 1985.

[26] B. Chor and E. Kushilevitz, "Secret sharing over infinite domains," in *Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto '89*, G. Brassard, Ed., Santa Barbara, CA, Aug. 20–24, 1989, pp. 299–306. Berlin: Springer-Verlag, 1990.

[27] R. A. Croft and S. P. Harris, "Public-key cryptography and re-usable shared secrets," 1986 IMA Conference on Cryptography and Coding, Cirencester, England, in *Cryptography and Coding*, H. J. Beker and F. C. Piper, Eds., pp. 255–268, Oxford: Clarendon Press, 1989.

[28] 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. Los Angeles: IEEE Computer Society Press, 1980.

[29] Y. G. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto '89*, G. Brassard, Ed., Santa Barbara, CA, Aug. 20–24, 1989, pp. 307–315. Berlin: Springer-Verlag, 1990.

[30] M. De Soete, "Geometric threshold schemes," presented at "Course on Geometries, Codes and Cryptography, organized by the *Centre International des Sciences Mécaniques*, June 19–23, 1989, Udine, Italy, to appear in *Lecture Notes* of the course.

[31] M. De Soete, J. Quisquater, and K. Vedder, "A signature with shared verification scheme," in *Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto '89*, G. Brassard, Ed., Santa Barbara, CA, Aug. 20–24, 1989, pp. 253–262. Berlin: Springer-Verlag, 1990.

[32] M. De Soete and K. Vedder, "Some new classes of geometric threshold schemes," in *Lecture Notes in Computer Science 330; Advances in Cryptology: Proc. Eurocrypt '88*, C. G. Günther, Ed., Davos, Switzerland, May 25–27, 1988, pp. 57–76. Berlin: Springer-Verlag, 1988.

[33] A. Ecker, "Tactical configurations and threshold schemes," preprint (available from author).

[34] P. Feldman, "A practical scheme for non-iterative verifiable secret sharing," *Proc. 28th Annu. Symp. Foundations of Computer Science*, Los Angeles, Oct. 12–14, 1987, pp. 427–437. Los Angeles: IEEE Computer Society Press, 1987.

[35] D. K. Gifford, "Cryptographic sealing for information secrecy and authentication," *Commun. ACM*, vol. 25, no. 4, pp. 274–286, April 1982.

[36] S. Harari, "Secret sharing systems," in *Secure Digital Communications*, G. Longo, Ed., Vienna: Springer-Verlag, pp. 105–110, 1983.

[37] I. Ingemarsson and G. J. Simmons, "How mutually distrustful parties can set up a mutually trusted shared secret scheme," *Intl. Assoc. Cryptologic Research (IACR) Newsletter*, vol. 7, no. 1, pp. 4–7, Jan. 1990.

[38] I. Ingemarsson and G. J. Simmons, "A protocol to set up shared secret schemes without the assistance of a mutually trusted party," in *Lecture Notes in Computer Science* 473; *Advances in Cryptology, Proc. Eurocrypt '90*, Aarhus, Denmark, May 21–24, 1990; I. Damgård, Ed., pp. 266–282. Berlin: Springer-Verlag, 1991.

[39] M. Ito, A. Saito, and T Nishizeki, "Secret sharing scheme realizing general access structure" (in English) *Proc. IEEE Global Telecommun. Conf., Globecom '87*, Tokyo, 1987, pp. 99–102. Washington, DC: IEEE Communications Soc. Press, 1987. Also appeared in *Trans. IECE Japan*, vol. J71-A, no. 8, 1988 (in Japanese).

[40] M. Ito, A. Saito, and T. Nishizeki, "Multiple assignment scheme for sharing secret," preprint (available from T. Nishizeki).

[41] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," IEEE Intl. Symp. Inform. Theory, Session B3 (Cryptography), Santa Monica, CA, February 9–12, 1981, *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[42] S. C. Kothari, "Generalized linear threshold scheme," in *Lecture Notes in Computer Science 196; Advances in Cryptology: Proc. Crypto '84*, G. R. Blakley and D. Chaum, Eds., Santa Barbara, CA, Aug. 19–22, 1984, pp. 231–241. Berlin: Springer-Verlag, 1985.

[43] K. Koyama, "Cryptographic key sharing methods for multi-groups and security analysis," *Trans. IECE Japan*, vol. E66, no. 1, pp. 13–20, 1983.

[44] C. S. Laih, L. Harn, and J. Y. Lee, "Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space," in *Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto '89*, G. Brassard, Ed., Santa Barbara, CA, Aug. 20–24, 1989, pp. 286–298. Berlin: Springer-Verlag, 1990.

[45] C. S. Laih, J. Y. Lee, and L. Harn, "A new threshold scheme and its applications in designing the conference key distribution cryptosystem," *Infor. Processing Lett.*, vol. 32, pp. 95–99, 1989.

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

[47] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, Sept. 1981.

[48] C. Meadows, "Some threshold schemes without central key distributors," *Congressus Numerantium*, vol. 46, pp. 187–199, 1985.

[49] M. Merritt, "Key reconstruction," in *Advances in Cryptology: Proc. Crypto '82*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds., Santa Barbara, CA, Aug. 23–25, 1982, pp. 321–322. New York: Plenum Press, 1983.

[50] M. Mignotte, "How to share a secret," Workshop on Cryptography, Burg Feuerstein, Germany, March 29–April 2, 1982, in *Cryptography*, vol. 149, T. Beth, Ed., pp. 371–375. Berlin: Springer-Verlag, 1983.

[51] R. von Randow, "The bank safe problem," *Discrete Appl. Math.*, vol. 4, pp. 335–337, 1982.

[52] P. J. Schellenberg and D. R. Stinson, "Threshold schemes from combinatorial designs," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 5, pp. 143–160, 1989.

[53] A. Shamir, "How to share a secret," *Massachusetts Institute of Technology Technical Report MIT/LCS/TM-134*, May 1979. (See also *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.)

[54] G. J. Simmons, "Robust shared secret schemes or 'how to be sure you have the right answer even though you don't know the question'," 18th Annu. Conf. Numerical Mathematics and Computing, Sept. 29–Oct. 1, 1988, Winnipeg, Manitoba, Canada; appeared in *Congressus Numerantium*, vol. 68, pp. 215–248, May 1989.

[55] G. J. Simmons, "How to (really) share a secret," in *Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto '88*, S. Goldwasser, Ed., Santa Barbara, CA, Aug. 21–25, 1987, pp. 390–448. Berlin: Springer-Verlag, 1990.

[56] G. J. Simmons, "Sharply focused sets of lines on a conic in PG(2,q)," presented at 20th Southeastern International Conference on Combinatorics, Graph Theory and Computing, Boca Raton, FL, Feb. 20–24, 1989; in *Congressus Numerantium*, vol. 73, pp. 181–204, Jan. 1990.

[57] G. J. Simmons, "Prepositioned shared secret and/or shared control schemes," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt '89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10–23, 1989, pp. 436-467. Berlin: Springer-Verlag, 1990.

[58] D. R. Stinson and S. A. Vanstone, "A combinatorial approach to threshold schemes," in *Lecture Notes in Computer Science 293; Advances in Cryptology: Proceedings of Crypto '87*, C. Pomerance, Ed., Santa Barbara, CA, Aug. 16–20, 1987, pp. 330–339. Berlin: Springer-Verlag, 1988.

[59] D. R. Stinson and S. A. Vanstone, "A combinatorial approach to threshold schemes," *SIAM J. Disc. Math*, vol. 1, no. 2, pp. 230–236, May 1988. (This is an expanded version of the paper that appeared in *Lecture Notes in Computer Science 293; Advances in Cryptology: Proceedings of Crypto '87*, C. Pomerance, Ed., Santa Barbara, CA, Aug. 16–20, 1987, pp. 330–339. Berlin: Springer-Verlag, 1988.)

[60] M. Tompa and H. Woll, "How to share a secret with cheaters," in *Lecture Notes in Computer Science 263; Advances in Cryptology: Proc. Crypto '86*, A. M. Odlyzko, Ed., Santa Barbara, CA, Aug. 11–15, 1986, pp. 133–138. Berlin: Springer-Verlag, 1987.

[61] T. Uehara, T. Nishizeki, E. Okamoto, and K. Nakamura, "Secret sharing systems with matroidal schemes," *Trans. IECE Japan*, vol. J69-A, no. 9, pp. 1124–1132, 1986 (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 *Technical Report TRECIS8601*, Department of Electronic Communications, Tohoku University, 1986.

[62] H. Unterwalcher, "Threshold schemes based on systems of equations," *Österreichische Akademie der Wissenschaften, Math.-Natur. Klasse, Sitzungsber. Abt. II*, vol. 196 (4–7), Vienna, pp. 171–180, 1987.

[63] H. Unterwalcher, "A department threshold scheme based on algebraic equations," in *Contributions to General Algebra 6*, Dedicated to the memory of Wilfried Nöbauer, pp. 287–298. Stuttgart, Federal Republic of Germany: Vienna, Verlag B. G. Teubner, 1988.

[64] W. D. Wallis, "Not all perfect extrinsic secret sharing schemes are ideal," *Australasian J. Combinatorics*, vol. 2, pp. 237–238, Sept. 1990.

[65] H. Yamamoto, "On secret sharing schemes using (k, L, n) threshold scheme," *Trans. IECE Japan*, vol. J68-A, no. 9, pp. 945–952, 1985 (in Japanese); also published as "Secret sharing system using (k, L, n) threshold scheme," *Electronics and Communications in Japan*, part 1, vol. 69, no. 9, pp. 46–54, 1986.

[66] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Inform. Theory*, vol. IT-32, no. 3, pp. 387–393, May 1986.

[67] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. Inform. Theory*, vol. IT-35, no. 3, pp. 572–578, May 1989.

[68] A. C. Yao, "How to generate and exchange secrets," in *27th Annual Symp. Foundations of Computer Sci.*, Toronto, Canada, Oct. 27–29, 1986, pp. 162–167. Los Angeles: IEEE Computer Society Press, 1986.