Computers & Security, 13 (1994) 69-78

Refereed paper

The breadth of Shamir's secret-sharing scheme

Ed Dawson and Diane Donovan*

Information Security Research Centre, Faculty of Information Technology, Queensland University of Technology, Brisbane, Queensland 4001, Australia

In 1979 Shamir and Blakley introduced the concept of secret sharing through threshold schemes. Their models were based on polynomials and finite geometries. Since 1979 many researchers have taken the basic concept of a threshold scheme and used other mathematical structures to adapt threshold schemes to meet the needs of many practical situations. In this paper the authors take Shamir's construction and show how it can be used to realize the adapted models. In particular, the authors give new constructions for multipart, multilevel, democratic and prepositioned schemes. It will also be demonstrated how known methods for detecting cheaters and disenrolling participants can be incorporated into Shamir's scheme.

Keywords: Secret-sharing schemes, Threshold schemes, Polynomial interpolation, Security and protection, Data encryption, Distributed systems.

1. Introduction

In the open system environment it is vital that access be restricted to confidential information on the system and to certain nodes in the system. This can be done through a cryptographic key, knowledge of which allows access. Cryptographic key management systems need to possess a high degree of security. In addition, key management systems need to be highly flexible. This can be achieved by taking a secret key and sharing it between a number of participants. The participants could be anything from a node on a network to executives within an organization.

For example, one may take the cryptographic key to be a number K in the range $0, ..., N-1$. This key can then be divided into n numbers which sum to K modulo N. These n numbers are distributed to the participants as shares. When one wishes to reconstruct the key, the participants divulge their numbers, the sum is taken and K is recovered. If $n-1$ participants collaborate, then they have no information about the secret whatsoever, since each of the numbers from $0, ..., N-1$ is equally likely to be the secret. Hence the scheme has a high degree of security. However, if one of the participants is incapacitated, then there is no way of recovering the key. Consequently, this scheme is not flexible enough to meet the needs of most real world situations.

Shamir [1] and Blakley [2] addressed this problem in 1979 when they introduced the concept of a threshold scheme. A t-out-of-n threshold scheme is a method whereby n pieces of information, called *shares*, in a secret key K are distributed in such a way that

*Present address: Mathematics Department, The University of Queensland, Brisbane, Queensland 4072, Australia.

- the secret can be reconstructed from knowledge of any t or more shares; and

- the secret cannot be reconstructed from knowledge of fewer than t shares.

The parameter t is often referred to as the *threshold* of the scheme. A threshold scheme is said to be *perfect* if a participant, or an unauthorized group of participants, has no advantage in guessing the secret over an outsider. Therefore a t-out-of-n threshold scheme is perfect if

- knowledge of fewer than t shares provides no information about K.

The key K is selected from a key space $\mathcal{K}$ which is taken to be finite.

One may use the entropy of a key to define a threshold scheme formally. Denning [3] defines the entropy of a message as a function H of the probability distribution over the set of all possible messages. Let $X_1, \ldots, X_n$ be n possible messages occurring with probabilities $p(X_1), \ldots, p(X_n)$, where $\Sigma_{i=1}^{n} p(X_i) = 1$. The *entropy* of a given message X is defined to be the weighted average

$$H(X) = \sum_{i=1}^{n} p(X_i) \log_2 \left(\frac{1}{p(X_i)} \right)$$

Using the entropy function, a perfect t-out-of-n threshold scheme is a scheme in which the secret key K is divided into n pieces of information $s_1, \ldots, s_n$ in such a way that for any set of t indices $\{i_1, \ldots, i_t\}$

(1) $H(K|s_{i_1}, \ldots, s_{i_t}) = 0$, and

(2) $H(K) = H(K|s_{i_1}, \ldots, s_{i_{t-1}})$,

where $H(K|s_{i_1}, \ldots, s_{i_j})$ denotes the conditional entropy in K given knowledge of $s_{i_1}, \ldots, s_{i_j}$.

Shamir [1] and Blakley [2] gave methods for constructing threshold schemes from mathematical structures. Shamir used the structural characteristics of polynomials, while Blakley used the properties of finite geometries. This paper will follow the path suggested by Shamir and show how his ideas can be developed to produce secure and flexible secret-sharing schemes. We shall demonstrate how the known methods for detecting cheaters can be applied to Shamir's scheme, as well as giving new ideas for the disenrolment of participants. This paper also documents new constructions for multipart, multilevel, democratic and prepositioned schemes.

2. Shamir's construction

Shamir's scheme [1] is based on polynomial interpolation: given a set of t points $\{(x_1, y_1), \ldots, (x_t, y_t)\}$, where the x_is are all distinct, in a two-dimensional plane, there is a unique polynomial $f(x)$ of degree $t-1$ on these points. He constructed a t-out-of-n threshold scheme in which the secret is taken to be the value $f(0)$ for some function $f(x)$, and the shares are taken to be the values $f(i)$, for $i = 1, \ldots, n$. It follows that any set of t shares can be used to recover the polynomial and hence the secret key.

More formally, one may construct a t-out-of-n threshold scheme as follows. The underlying field is taken to be Z_q for some large prime $q \geq n+1$. All arithmetic will be done modulo q. A key K is randomly chosen from a uniform distribution over the integers Z_q. Then coefficients $a_1, \ldots, a_{t-1}$ are also randomly chosen from Z_q. The polynomial

$$f(x) = K + a_1 x + \ldots + a_{t-1} x^{t-1},$$

of degree $t-1$, is taken to be a function which reveals the secret key K. The n participants in the scheme are labelled P_1 to P_n. The share distributed to participant P_i is the values $f(i)$. If a group, $P_{i_1}, \ldots, P_{i_t}$, of t participants wants to recover the secret key, then they may use their t ordered pairs $(i_j, f(i_j))$, for $j = 1, \ldots, t$, to obtain a system of t linear equations,

$$a_0 + a_1(i_1) + a_2(i_1)^2 + \ldots + a_{t-1}(i_1)^{t-1} = f(i_1)$$

$$a_0 + a_1(i_2) + a_2(i_2)^2 + \ldots + a_{t-1}(i_2)^{t-1} = f(i_2)$$

$$\bullet$$

$$\bullet$$

$$\bullet$$

$$a_0 + a_1(i_t) + a_2(i_t)^2 + \ldots + a_{t-1}(i_t)^{t-1} = f(i_t)$$

Since each of the i_js were distinct, Lagrange interpolation can be used and $f(x)$ recovered by evaluating

$$f(x) = \sum_{s=1}^{t} f(i_s) \prod_{1 \le j \le t, j \ne s} \frac{(x - i_j)}{(i_s - i_j)} \bmod q.$$

Of course, once $f(x)$ is known K can be obtained by evaluating $f(0)$. However, as pointed out by Stinson [4], the participants do not need to know the whole polynomial. They only require the value of the constant term $K = f(0)$. Hence the participants need only compute the expression

$$K = (-1)^{t-1} \sum_{s=1}^{t} f(i_s) \prod_{1 \le j \le t, j \ne s} \frac{i_j}{(i_s - i_j)} \bmod q.$$

Suppose that a set of $t-1$ participants $\{P_{i_1}, \ldots, P_{i_{t-1}}\}$ collude and try to recover the secret. They will have a system of $t-1$ linear equations in t unknowns. They can obtain a tth equation by guessing K_0 and set $f(0) = K_0$, for any value $K_0 \in Z_q$. Now they have a system of t equations in t unknowns and once again, by Lagrange interpolation, this system of equations has a unique polynomial of degree $t-1$ as a solution. Hence for each value $K_0 \in Z_q$ there is a unique polynomial which satisfies the t equations. Thus knowledge of $t-1$ shares provides no information about the secret key K, so that the scheme is perfect.

In the above scheme the assignment of the values 1, ..., n to the participants P_1, ..., P_n need not be carried out in secret. However, it will be shown in the next section that in many situations it may be desirable to assign an arbitrary value x_i to participant P_i and then assign him the share $f(x_i)$.

3. Enhanced security

Methods have been suggested which can enhance the security of a secret-sharing scheme. Two such methods will be discussed in this section. First, this section will deal with the identification of cheaters, and then methods will be suggested which can be used to disenrol participants.

Assume that a t-out-of-n threshold scheme based on Shamir's construction has been set up; that is, a number $K \in Z_q$ has been chosen as the secret and a polynomial $f(x)$ of degree $t-1$ with constant coefficient K has been chosen. The participants are labelled P_i, for $i = 1$, ..., n, and participant P_i is given $f(i)$ as his share. Tompa and Woll [5] pointed out that if a participant P_i wants to cheat $t-1$ of the other participants, then all that is necessary is to find a polynomial $g(x)$ of degree at most $t-1$ such that $g(0) = -1$ and $g(j) = 0$ for all $j \ne i$. This polynomial can be found by Lagrange interpolation. Having done this, the participant takes his share $f(i)$ and adds $g(i)$ to it. When it is time to reconstruct the secret, participant P_i inputs the share $f(i) + g(i)$. The participants will reconstruct the polynomial $f(x) + g(x)$ and recover the constant coefficient $K - 1$. At this point the dishonest participant will be able to recover the secret. (Note: $g(0) = -1$ could be changed to $g(0) = -a$, for any a.) The other participants may not even know that they have a false secret, let alone know who cheated.

So it is certainly feasible for a group of participants to deceive the other participants by fabricating false shares. In addition to this, it would be easy for the administrator (some trusted authority) of the scheme to issue a false share and hence prevent the recovery of the key.

Tompa and Woll [5] suggested that Shamir's scheme could be modified to make it harder for a participant to cheat. They suggested that a participant P_i be given the share $f(x_i)$ for some arbitrary assignment of x_is, where all the x_is are distinct and not equal to 0. In this system participant P_i is given as his share both x_i and $f(x_i)$. In this way a group of cheaters must guess the value of x_i in order to instigate the above fraud. While such a scheme will detect a fraud, it cannot determine who the dishonest parties are. There is also a small probability that false shares may go undetected.

Simmons [6] suggested that the correct value of the secret key be verified by requiring an extra participant to use his share to validate the secret key. Brickell and Stinson [7] have addressed the problem of cheaters by requiring that each participant hold $n-1$ pieces of additional information which they can use to validate the shares tendered by each of the other participants. But this means that each participant must hold in total n pieces of secret information.

Karnin, Greene and Hellman [8] suggested that one simple solution to the identification of cheaters would be to use a one-way function to encrypt the key. This encrypted value may be stored in a public register. Once the participants recover a key, they can use the one-way function to verify that it is the correct key. However, in the event of a cheater, they have no way of detecting who is cheating. So, in addition, when the administrator creates the shares he may encrypt them using a one-way function and store these values in a public register. At the point of recovery, each of the participants inputs his share, and the encrypted version can be used to verify it. If it should transpire that each of the shares is validated by the one-way function but the secret is not, this indicates that the administrator was not so trustworthy. It should be noted that the democratic schemes described in Section 6 provide another method for overcoming the problem of an unreliable administrator.

Depending on the physical security requirements of the situation, any of the above features can easily be built into Shamir's scheme.

Alternatively, the security of a system may be reduced by one of the participants broadcasting his shares. The result would be that any $t-1$ of the remaining participants may collaborate and use the exposed share, together with their own, to determine the secret. In this situation the threshold is reduced from t to $t-1$. In order to keep the threshold level at t, the key must be changed and new shares distributed. One way to do this is to distribute new shares on a secure channel. However, setting up such a channel can be costly. Thus there is a need to develop systems which can be modified by the distribution of information on insecure channels. It should be understood that this information should not compromise the security of the scheme in any way. Blakley, Blakley, Chan and Massey [9] termed systems with this property schemes with disenrolment capabilities and outlined how to implement such schemes using finite geometric structures. It will be shown below that a disenrolment capability can be incorporated into Shamir's scheme.

Suppose that we have a t-out-of-n threshold scheme based on polynomials over the set $Z_q=\{0, 1, \ldots, q-1\}$. Further, assume it is necessary to design a scheme which allows for disenrolling up to L shares, where $(n-L \geq t)$. Initially, an administrator selects $L+1$ secrets $K_0, K_1, \ldots, K_L$ from the set Z_q as well as selecting $L+1$ polynomials $f_i(x)$ of degree $t-1$, for $i=0, \ldots, L$, where K_i is the constant coefficient of $f_i(x)$. The administrator generates n shares for each of the $L+1$ secrets. Participant P_j's share to secret K_i is s_{ji}, where $f_i(j)=s_{ji}$. Random numbers r_{ji}, for $j=1, \ldots, n$ and $i=1, \ldots, L$, are selected from Z_q. The random number r_{ji} is combined with the share s_{ji} to form s'_{ji}; that is, $s'_{ji}=s_{ji}+r_{ji}$. In this manner we use r_{ji} to mask the share s_{ji}. Initially, the administrator sends, over a secure channel, the $L+1$ shares s_{j0} and s'_{ji}, for $i=1, \ldots, L$, to participant P_j. In the first instance any t participants can use their shares, of the form s_{j0}, to derive the secret K_0. However, if one of the participants reveals his shares (we will assume for simplicity of notation that this is the first participant) the administrator can disenrol this person. This is achieved by the following procedure. The administrator changes the key to K_1 and broadcasts, on an open insecure channel, the random numbers r_{j1} for $j=2, \ldots, n$. Participant P_j, for $j=2, \ldots, n$, can use the random number r_{j1} to unmask s'_{j1} and recover the share s_{j1} to secret K_1. Hence any t of the remaining $n-1$ participants can combine their shares to derive K_1. However, the disenrolled participant is not able to derive share s_{11} without knowledge of r_{11}. Hence, this person can no longer participate in the scheme, unless the administrator broadcasts r_{11}. This procedure can be repeated and L participants can be disenrolled. It should be noted that, as well as disenrolment, the above scheme provides a method whereby an administrator can establish a new secret at any time. The information necessary to determine the new shares can then be broadcast on an insecure channel.

4. Information rate

If one lets $\mathscr{K}$ represent the key space from which the secret key K is chosen, then K can be represented by a bit string of length $\log_2|\mathscr{K}|$. Likewise, if $\mathscr{S}_i$ is used to denote the set of possible shares which may be distributed to participant P_i for $i=1, \ldots, n$, then the share distributed to that participant may be represented by a bit string of length $\log_2|\mathscr{S}_i|$. The information rate for participant P_i is the ratio

$$\rho_i=\frac{\log_2|\mathscr{K}|}{\log_2|\mathscr{S}_i|}$$

The information rate ρ for a perfect threshold scheme is taken to be the minimum of these values. That is, the information rate for the scheme is

$$\rho=\min\{\rho_i|1\leq i\leq n\}.$$

If we have the optimal situation when $\rho=1$, then the scheme is said to be *ideal.*

Since the key space and the share space for Shamir's scheme is the set Z_q, where q is a large prime, Shamir's scheme is ideal.

5. General secret-sharing schemes

In a t-out-of-n threshold scheme it is infeasible for the secret key to be recovered from $t-1$ shares. However, it can be recovered even when $n-t$ of the shares have been lost. There are many situations in which it is desirable to have a more flexible arrangement for recovering the secret. Given a set of n participants, one may wish to designate certain authorized groups of participants who can use their shares to recover the secret key. Then one talks about a general secret-sharing scheme as a method whereby n shares are assigned to a secret key K, and the secret can be reconstructed only from certain authorized groups of shares. It must be infeasible for the secret key to be recovered from an unauthorized group of shares.

Let $\mathscr{P}$ denote the set of participants and let Γ denote the set of subsets of $\mathscr{P}$ which have the property that the shares held by the participants from a subset can be combined and the secret recovered; that is, the elements of Γ are the authorized groups of participants. Then Γ is said to be the *access structure* for the secret-sharing scheme and the elements of Γ are termed the *authorized subsets.* It is assumed that if $B\in\Gamma$, then for all $A\subseteq\mathscr{P}$ where $B\subseteq A$, $A\in\Gamma$. Schemes with this property are termed *monotone.* Further, if $B\in\Gamma$ and for all $A\subset B$, $A\notin\Gamma$, then B is termed a *minimal authorized subset.* The set of minimal authorized subsets of Γ forms the *basis* of Γ and is denoted by Γ_0. Often one will specify the basis and use it to uniquely determine the access structure. Formally, Γ is said to be the closure of Γ_0, or

$$\Gamma=\{A\subseteq\mathscr{P}\,|B\subseteq A, \text{where } B\in\Gamma_0\}.$$

For example, if the set of participants is $\mathscr{P}=\{P_1, P_2, P_3, P_4, P_5\}$, then one may take a basis for an access structure Γ to be the set

$$\Gamma_0=\{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3\}, \{P_1, P_4, P_5\}\}.$$

In this case the minimal authorized subsets are the sets $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_1, P_3\}$, $\{P_1, P_4, P_5\}$ and the access structure is the set $\Gamma=\{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1,$

$P_3\}$, $\{P_1, P_4, P_5\}$, $\{P_1, P_2, P_3\}$, $\{P_1, P_2, P_4\}$, $\{P_1, P_2, P_5\}$, $\{P_1, P_4, P_3\}$, $\{P_1, P_5, P_3\}$, $\{P_2, P_4, P_3\}$, $\{P_2, P_5, P_3\}$, $\{P_1, P_2, P_4, P_5\}$, $\{P_1, P_3, P_4, P_5\}$, $\{P_2, P_3, P_4, P_5\}$, $\{P_1, P_2, P_3, P_4\}$, $\{P_1, P_2, P_3, P_5\}$, $\mathscr{P}\}$

A scheme is a *perfect secret-sharing scheme* realizing the access structure Γ if

(1) an authorized subset of participants, $A \in \Gamma$, can reconstruct the secret key from their shares; and

(2) if an unauthorized subset of participants, $A \notin \Gamma$, can determine nothing about the secret key from their shares.

Formally, the access structure Γ is realized by a perfect secret-sharing scheme if the secret key K is divided into n pieces of information $s_1, \ldots, s_n$ in such a way that

(1) $H(K|S_A) = 0$, where S_A is the set of shares held by the participant in a set $A \in \Gamma$; and

(2) $H(K) = H(K|S_A)$, where S_A is a set of shares held by the participants of a set $A \notin \Gamma$.

Benaloh and Leichter [10] showed that no matter what the access structure is, it is always possible to construct a general secret-sharing scheme based on the traditional threshold scheme proposed by Shamir. To demonstrate this, we take a general secret-sharing scheme with an arbitrary access structure Γ. The elements of Γ are the authorized groups of participants whose shares can be used to reconstruct the secret, and the minimal sets are the authorized groups no subset of which can recover the secret. We shall assume that each participant belongs to at least one minimal set. An administrator selects a secret key K and labels the participants $P_1, \ldots, P_n$. A minimal set A based on a set of s participants is chosen and a polynomial $f_A(x)$ of degree $s-1$ with constant coefficient K is assigned to A. Let participant P_i be a member of this minimal set. Participant P_i is given the share $f_A(i)$. This procedure is repeated for each participant in A and then for each minimal set in Γ. Essentially, we have constructed a series of s-out-of-s threshold schemes, one for each minimal set. (Note that the number s may vary, depending on the size of the minimal set.) It is easy to see that any authorized group will be able to recover the secret.

However, since a participant requires a share for each minimal set to which he belongs, he may be required to hold multiple shares. There is a simple method for reducing this number. Let M be a subset of the participants, where $|M| = m$. Further, suppose that any s of the participants from M form a minimal set of the access structure. That is, any s of the participants from M can recover the secret. There are

$$\binom{m}{s} = \frac{m!}{s!(m-s)!}$$

minimal sets with participants chosen from M. These $\binom{m}{s}$ sets are all assigned the same polynomial and shares are distributed accordingly. In this manner an s-out-of-m threshold scheme for the participants of M has been constructed. This process is then repeated until all minimal sets in the access structure are associated with some polynomial, where each of the polynomials has the same constant coefficient. In this fashion, a general secret-sharing scheme can be thought of as a series of s-out-of-n threshold schemes.

We may take the basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3\}, \{P_1, P_4, P_5\}\}$ for the access structure given above and demonstrate how this method works. In such a system, participants P_1, P_2, P_3 are assigned a 2-out-of-3 threshold scheme, while participants P_1, P_4, P_5 are assigned a 3-out-of-3 threshold scheme. In order to implement the scheme with the above minimal sets, polynomials $f(x)$ and $g(x)$, of degrees one and two respectively, each with the same constant coefficient K, are required. The result is that the shares of participants P_1, P_2 and P_3 are determined by the polynomial $f(x)$, while the shares of participants P_1, P_4 and P_5 are determined by the polynomial $g(x)$. Participant P_1 has a share in each polynomial while the other participants have only one share each.

There are two types of general access structure which have been studied in detail. In the first of these the participants are divided into groups and the secret can be recovered only when the prescribed number of participants from each group concur. In the second the access structure satisfies a hierarchical structure; that is, one in which certain groups of shares can be used to replace the share of a participant at a higher level. These particular types of scheme are termed multipart and multilevel schemes, respectively.

First, let us consider a multipart scheme. For simplicity, let us assume the participants are divided into two compartments, where the threshold in each compartment is the same. Name these compartments A and B. In a *multipart scheme* a secret key is selected and shares assigned to this secret such that

(1) any set of t participants from compartment A, together with any set of t participants from compartment B, can combine their shares and recover the secret; but in addition

(2) less than t participants from any one compartment, together with any number of participants from the other compartment, cannot recover the secret uniquely.

Multipart schemes have been constructed previously by Simmons [6, 11], using finite geometric structures, and by Brickell [12], using bases in a vector space. It will be shown below that multipart schemes can be constructed using polynomials as well.

Assume that the participants are divided into two compartments and each compartment contains m participants. The participants in compartment A are labelled $P_{A1}, \ldots, P_{Am}$, and the participants in compartment B are labeled $P_{B1}, \ldots, P_{Bm}$. An administrator selects two polynomials, of degree $t-1$, denoted by $f_A(x)$ and $f_B(x)$. Assume the constant coefficients for these polynomials are K_A and K_B, respectively. The secret key shall be the number K, where $K=K_A+K_B$. For each $i=1, \ldots, m$, the administrator gives participant P_{A_i} the share $f_A(i)$. Similarly, participants P_{B_i} are given the shares $f_B(i)$. When t participants from any one group combine their shares they obtain the polynomial $f_C(x)$, for $C=A$ or B. When both polynomials are obtained, K can be recovered. However, K cannot be recovered through knowledge of only one of K_A or K_B. Hence the scheme satisfies the properties of a multipart scheme with two compartments. Clearly, these ideas can be generalized to construct schemes on more than two compartments and schemes in which the threshold differs from one compartment to the next.

We now turn to multilevel schemes. In a *multilevel* or *hierarchical scheme* pieces of related information, the shares, to a secret key K, are distributed to n_r individuals of level r, where $r=1, \ldots, l$. It is assumed that the secret can be recovered from the shares of t_l participants of level l. However, if a participant of level l is unavailable, then their share may be replaced by any set of t_{l-1} participants of level $l-1$. Similarly, if a participant of level $l-1$ is unavailable their share can be replaced by any t_{l-2} participants of level $l-2$, and so on. Multilevel schemes have been constructed previously by Beutelspacher and Vedder [13] and Simmons [6, 11], using finite geometric structures, and by Brickell [12], using bases in a vector space. It will also be shown below that such schemes can be constructed using polynomials.

For ease of exposition, let us assume that there are two levels. We shall demonstrate how Shamir's original ideas can be used to construct a two-level scheme. The participants are assigned the appropriate ranking. The participants in level one are labelled $P_{1,1}$ to P_{1,n_1} and those in level two are labelled $P_{2,1}$ to P_{2,n_2}. An administrator selects a secret key K and a polynomial $f_2(x)$, of degree t_2-1, with constant coefficient K. The participants in level two, the highest level, are given the shares

$f_2(1)$, ..., $f_2(n_2)$. The administrator then selects a polynomial $f_1(x)$, of degree $t_1 - 1$, with constant coefficient $f_2(n_2 + 1)$. He then distributes the share $f_1(i)$ to participant P_{1i}, for each $i = 1, ..., n_1$. If t_2 participants from level two come together they can combine their shares and uniquely determine the polynomial $f_2(x)$. In this manner they can recover the secret key. However, if only $t_2 - 1$ participants are available, then a group of t_1 participants at level one can combine their shares and determine a number which corresponds to the point $(n_2 + 1, f_2(n_2 + 1))$. We now have t_2 points on the polynomial $f_2(x)$, making it possible to recover the secret uniquely.

It should be noted that there is a small probability that the share $f_1(i)$ for participant $P_{1,i}$ at level one is on the polynomial $f_2(x)$. This may allow $P_{1,i}$ to masquerade as a participant at level two. However, it is a simple procedure for the administrator to avoid this by comparing shares prior to distribution. If there is such a collision of shares, the administrator can select another polynomial.

The two-level scheme described above can be generalized to r levels. In this case the participants of level r can derive the secret. The participants at level j, for $j = 1, ..., r - 1$, will determine a point on the polynomial corresponding to level $j + 1$. In this fashion, a set of participants at level j can replace a participant at level $j + 1$.

6. Democratic schemes

In each of the situations discussed so far, it has been assumed that there exists an authority trusted by all parties to choose the secret, determine the shares and distribute these shares privately to the participants. Such schemes have been termed *autocratic*. In Section 3, we briefly mentioned the possibility of placing checks on the administrator to ensure that he carries out the above process honestly. However, there is an alternative. The participants in a scheme may determine the secret amongst themselves and privately assign shares to this secret, thereby doing away with the need for an administrator.

However, the problem is: how does one go about setting up such a scheme? Ingemarsson and Simmons addressed this problem in 1991 [14], and designed a democratic scheme. In a *democratic scheme* the participants agree on a common key space. From this each participant selects a personal secret. These secrets are fed into a controlling mechanism and a master secret determined. The master secret could be, for example, the sum of the personal secrets. Each participant assigns shares to his personal secret and distributes one share each to the other participants. At this point each participant holds $n - 1$ shares, one from each of the other participants. When an authorized group of participants come together, they hold enough information to determine each personal secret and this, when fed into the controlling mechanism, can be used to determine the master secret. Ingemarsson and Simmons's original construction was given in terms of maximum distance separable codes and finite geometric structures. As we shall show below, a similar construction can also be given in terms of polynomials.

The participants are labelled $P_1, ..., P_n$. The participants decide on a set of numbers Z_q to be the set of possible keys. Each participant P_j selects a number K_j from this set. This number is fed into a controlling mechanism which computes $\Sigma_{j=1}^{n} K_j = K$. The number K is taken to be the master key. Participant P_j selects a polynomial $f_j(x)$ of degree $t - 1$ with constant coefficient K_j; that is,

$$f_j(x) = K_j + a_{j,1}x + a_{j,2}x^2 + \ldots + a_{j,t-1}x^{t-1}.$$

Now participant P_j evaluates $f_j(i)$ for $i = 1, ..., n$, $(i \neq j)$, and distributes $f_j(i)$ to participant P_i. When t participants come together they know their own personal key K_j and hold shares in each of the $n - t$ polynomials chosen by the absent participants. Therefore, they can determine these $n - t$ polynomials and thus the personal keys. Once the keys are fed into the controlling mechanism the secret K is recovered.

7. Prepositioned schemes

When one is setting up a communications network there may not be an immediate need for a secret-sharing scheme. However, no situation is ever static and one may wish to provide for the possibility of an access control scheme in the future. In these circumstances one may set up a *prepositioned secret-sharing scheme* in which a secret is selected, shares in the secret assigned, but, in addition, one determines an extra piece of information which must be combined with the shares before the secret can be recovered. So, in a prepositioned scheme, the participants are unable to recover the secret from their shares until such time as the scheme is activated by the administrator communicating additional information. Simmons [6] first introduced the idea of a prepositioned scheme in 1987.

Simmons suggested that one may use a DES (Data Encryption Standard) key in the construction of a prepositioned scheme. A secret key K is selected and then a DES key is used to encode it. The participants are assigned shares in the DES key and they may recover it at any time. However, it is of no value to them until they receive the ciphertext, which is the encrypted version of K. The ciphertext is sent only when one wants to activate the scheme. Once the participants receive the ciphertext they can use the DES key to encrypt it and hence they have the secret key K. Obviously, such a system can be built around Shamir's scheme.

Alternatively, one may use Shamir's scheme as follows to construct a prepositioned scheme. A number K is chosen to be the secret key, and a polynomial $f(x)$ of degree $t-1$ is chosen such that $f(x_0)=K$, for some x_0. For each i the participant P_i is assigned the value x_i. The x_is must all be distinct and not equal to x_0. The value $f(x_i)$ is calculated and distributed to participant P_i as his share. When t participants come together they can combine their shares and obtain the polynomial $f(x)$. However, they must be given the value x_0 in order to recover the secret.

8. Conclusion

This paper highlights the usefulness of Shamir's original t-out-of-n threshold scheme. As has been shown in this paper, polynomials modulo a prime q can be used to implement a secret-sharing scheme over any general access structure. As well, methods for detecting cheaters have been suggested, and disenrolment of participants is addressed. However, a secret-sharing scheme must possess additional properties before it can be accepted as a model for a robust key management system. These properties are:

(1) The method used to generate the secret and the shares should be efficient.

(2) The decoding algorithm used to recover the secret should be efficient.

(3) The scheme should be adaptable, in that it should be simple to change the access structure.

Secret-sharing schemes based on polynomials, as described in this paper, satisfy all three of these properties. For example, if the secret is a 56-bit DES key, one may select the prime q to be the first prime larger than 2^{56}. (This is the prime $q=72057594037928017$). In order to generate shares, recover the secret key and change the access structure, one only needs access to efficient packages to generate random numbers and to carry out multiprecision arithmetic modulo q. Property (1) is satisfied since a random number generator allows one to select the coefficients of the polynomials. The multiprecision arithmetic package provides an efficient method for generating the shares. Property (2) is satisfied since the multiprecision arithmetic package, in conjunction with Lagrange interpolation, provides an efficient method for solving a system of linear equations. As has been shown in this paper, secret-sharing schemes based on polynomials make it relatively easy to adapt a scheme to allow for changes in the access structure. Essentially, changing the access structure requires only the capability of adding new shares or generating more random polynomials. Property (3) is therefore satisfied. It has been shown that Shamir's scheme meets all these requirements and can be used to implement a versatile, robust secret-sharing scheme.

Acknowledgment

The research in this paper has been funded in part by a Meritorious Projects Grants Scheme at the Queensland University of Technology and in part by the Cooperative Research Centres Program through the Department of the Prime Minister and Cabinet of the Commonwealth Government of Australia. The second author also wishes to acknowledge the support of a Postdoctoral Fellowship at the Queensland University of Technology.

References

[1] A. Shamir, How to share a secret, *Comm. ACM*, 22(11) (1979) 612–613.

[2] G.R. Blakley, Safeguarding cryptographic keys, *Proc. AFIPS 1979 Natl. Comput. Conf., New York*, 48 (1979) 313–317.

[3] D.E. Denning, *Cryptography and Data Security*, Addison-Wesley, 1982.

[4] D.R. Stinson, An explication of secret sharing schemes, *Designs, Codes and Cryptography*, 2 (1992) 357–390.

[5] M. Tompa and H. Woll, How to share a secret with cheaters, *J. Cryptol.*, 1 (1988) 133–138.

[6] G.J. Simmons, How to (really) share a secret, in S. Goldwasser (ed.), *Lecture Notes on Computer Science 403; Advances in Cryptology: Proc. Crypto 1988, Santa Barbara, CA, Aug. 1988*, Springer-Verlag, Berlin, 1990, pp. 390–448.

[7] E.F. Brickell and D.R. Stinson, The detection of cheaters in threshold schemes, *Siam J. Discrete Math.*, 4 (1991) 502–510.

[8] E.D. Karnin, J.W. Greene and M.E. Hellman, On secret sharing systems, *Proc. IEEE Int. Symp. Inform. Theory, Santa Monica, CA, Feb. 1981; IEEE Trans. Inform. Theory*, IT-29(1) (1983) 35–41.

[9] B. Blakley, G.R. Blakley, A.H. Chan and J.L. Massey, Threshold schemes with disenrollment, *Proc. Crypto 1992, Santa Barbara, CA, Aug. 1992*, 13-1–13-4.

[10] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, in S. Goldwasser (ed.), *Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto 1988, Santa Barbara, CA, Aug. 1988*, Springer-Verlag, Berlin, 1990, pp. 27–35.

[11] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their applications, in *Contemporary Cryptology, The Science of Information Integrity*, IEEE Press, Piscataway, 1991, pp. 441–497.

[12] E.F. Brickell, Some ideal secret sharing schemes, *J. Comb. Math. Comb. Comput.*, 6 (1989) 105–113.

[13] A. Beutelspacher and K. Vedder, Geometric structures as threshold schemes, *1986 IMA Conf. on Cryptography and Coding, Cirencester, England*, also in H.J. Beker and F.C. Piper (eds.), *Cryptography and Coding*, Clarendon Press, Oxford, 1989, pp. 255–268.

[14] I. Ingemarsson and G.J. Simmons, A protocol to set up shared secret schemes without the assistance of a mutually trusted party, in I. Damgård (ed.), *Advances in Cryptography, Proc. Eurocrypt '90*, Springer-Verlag, Berlin, 1991, pp. 266–282.