THRESHOLD SCHEMES WITH DISENROLLMENT

Bob Blakley[1], G.R. Blakley[2], A.H. Chan[3] and J.L. Massey[4]

[1] Entry Systems Division, IBM Corporation, Austin, TX 78758
[2] Department of Mathematics, Texas A&M University, College Station, TX 77843-3368
[3] College of Computer Science, Northeastern University, Boston, MA 02115.
Agnes Chan's work was supported by MITRE Sponsored Research Program.
[4] Swiss Federal Institute of Technology, Zurich 8092, Switzerland

Abstract. When a shadow of a threshold scheme is publicized, new shadows have to be reconstructed and redistributed in order to maintain the same level of security. In this paper we consider threshold schemes with disenrollment capabilities where the new shadows can be created by broadcasts through a public channel. We establish a lower bound on the size of each shadow in a scheme that allows L disenrollments. We exhibit three systems that achieve the lower bound on shadow size.

1 Introduction

In safeguarding a secret, there are many situations where two or more guardians provide more security than only one. Common examples can be found in safe deposit boxes and in the control of nuclear weapons. In these cases, two keys are needed to activate the control mechanism; the ability to exercise shared control is lost if either key is lost or either key's owner is incapacitated. To guard against such a loss, copies of keys or instructions may be made and distributed to different parties. However, increasing the number of distributed copies increases the risk of some copy being compromised, thus reducing the security of the system. By distributing "shadows" of a shared secret (which can be used as a key),threshold schemes allow shared control without risking compromise of the secret.

Let S be a secret which needs to be protected. The secret S is concealed among n different shadows in such a way that:

1. For some threshold $t, t \leq n$, called the "threshold size", any t shadows determine the secret S.
2. No $t-1$ or fewer shadows uniquely determine the secret.

The secret S is secure against the collusion of any $t-1$ or fewer owners of shadows, and the scheme is protected against the loss of any $n-t$ shadows.

Blakley[1] published a (t, n) threshold scheme using hyperplanes. Shamir[7] proposed a threshold scheme using polynomials over a finite field. Various other

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 540-548, 1993.

schemes (using vector spaces, combinatorial designs, finite geometries and Reed-Solomon codes) exist [3, 4, 6, 9]. Schemes with the property that the disclosure of $t-$ 1or fewer shadows does not reveal any information about the secret are called *perfect* threshold schemes.

The disclosure of a shadow decreases the security against collusion of a threshold scheme since every $t-1$ remaining shadows, together with the disclosed shadow, determine the secret. Thus, the threshold is reduced from t to $t-1$. In order to maintain the same threshold t, the key must be changed and the shadows modified. One way to do this is to design a new (t,n) scheme where shadows are then distributed through secure channels. The security of the new system is not compromised if the new shadows are independent of the disclosed shadow. However, setting up the secure channels for distributing shadows can be expensive.

This paper considers schemes which distribute modifications to existing shadows through *insecure channels.* Such a scheme is said to have a *disenrollment capability.* Section 2 gives an information theoretic definition of threshold schemes with such a disenrollment capability and establishes a lower bound on the size of each shadow. Section 3 gives three examples of implementations that achieve the lower bound. The Brickell-Stinson Scheme[2] depends on the existence of a random number generator. The Nonrigid Hyperplane Scheme extends the original Blakley[1] Scheme to allow disenrollments. Finally, the Martin Scheme[5] makes use of threshold schemes with higher thresholds and reduces the cost of each public broadcast.

2 Information Theory and Lower Bound

A (t,n) threshold scheme distributes partially redundant shadows $S_1,\ldots,S_n$ among n users so that any t or more shadows uniquely determine the secret K. The random variable K representing the secret takes values in the space $\mathbb{K}$. The random variables $S_1,\ldots,S_n$ representing the shadows take values in a space $\mathbf{S}$. Using the entropy or "uncertainty" function $H(X)$ introduced by Shannon[8], we have the following definitions.

Definition 1. A (t,n) threshold scheme is a collection of random variables $(K,S_1,\ldots,S_n)$ such that for any $1\le i_1<i_2<\ldots<i_j\le n$,

$$H(K|S_{i_1},\ldots,S_{i_j})=0 \qquad \forall j\ge t, \tag{1}$$

$$H(K|S_{i_1},\ldots,S_{i_j})>0 \qquad \forall j<t. \tag{2}$$

Condition (1) says that every set of t or more shadows determines the secret uniquely, whereas condition (2) indicates that the secret cannot be uniquely determined by fewer than t shadows. A (t,n) threshold scheme is said to be *perfect* if

$$H(K|S_{i_1},\ldots,S_{i_j})=H(K) \qquad \forall j<t. \tag{3}$$

Condition (3) says that knowledge of fewer than t shadows does not reduce one's uncertainty about the secret.

Let us consider the case where one shadow, say S_1, is disclosed or invalidated. In order to maintain the threshold level at t, a new secret key has to be chosen and new shadows have to be constructed. If information on the new shadows can be distributed through a public channel without compromising the secrecy of the new key, then such a (t, n) threshold scheme is said to have a 1-fold disenrollment capability. If $L+1$ secrets can be chosen so that, while disenrolling L shadows successively, the broadcast public messages do not compromise the secrecy of the new key, then such a (t, n) threshold scheme is said to have an L-fold disenrollment capability. An information-theoretic model of such a scheme is given below.

Let $K_0, K_1, ..., K_L$ denote the $L+1$ secrets. Let $S_1, ..., S_n$ represent the shadows, any t of which determine the original secret key K_0. Without loss of generality we may assume that S_i corresponds to the shadow that is invalidated at the i-th disenrollment, $i = 1, ..., L$. Let $P_1, ..., P_L$ denote the public messages that are broadcast successively at each disenrollment step. Note that each P_i may include informations obtained from the revealed shadows, $S_1, \ldots, S_i$.

Definition 2. A (t, n) threshold scheme with L-fold disenrollment capability is a collection of random variables $(K_0, K_1, ..., K_L, S_1, ..., S_n, P_1, ..., P_L)$ such that for each $i, i = 0, ..., L$,

$$H(K_i | \Delta_i(k), P_1, ..., P_i) = 0 \qquad \forall k \geq t, \tag{4}$$

$$H(K_i | \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) > 0 \qquad \forall k < t, \tag{5}$$

where $\Delta_i(k) = \{S_{i_1}, ..., S_{i_k}\} \subseteq \{S_{i+1}, S_{i+2}, ..., S_n\}$.

Definition 3. A (t, n) threshold scheme with L-fold disenrollment capability is said to be perfect if

$$H(K_i | \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) = H(K_i) \qquad \forall k < t. \tag{6}$$

Let us assume that $H(K_i) = m$ bits. For a perfect (t, n) threshold scheme with L-fold disenrollment capability, conditions (4) and (6) can then be expressed in terms of mutual information as

$$I(K_i; \Delta_i(k), P_1, ..., P_i) = m \qquad \text{if} \quad k \geq t \tag{7}$$

$$I(K_i; \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) = 0 \qquad \text{if} \quad k < t \tag{8}$$

respectively, where we remind the reader that by definition,

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X).$$

In order to minimize the cost of distributing shadows through secure channels, we wish to minimize the number of bits required to encode each shadow. It is conceivable that a (t, n) threshold scheme with higher disenrollment capability requires higher overhead for encoding the shadows. The following theorem shows that this is indeed the case by establishing a lower bound on the number of bits required to encode a shadow that grows linearly with the number L of disenrollments.

Theorem 4. *Let $(K_0, K_1, ..., K_L, S_1, ..., S_n, P_1, ..., P_L)$ be a perfect (t, n) threshold scheme with L-fold disenrollment capability. If $H(K_i) = m$, for $i = 0, ..., L$, then*

$$H(S_j) \geq (L+1)m \qquad \forall j = 1, ..., n.$$

To prove the theorem, we first establish that the knowledge of previous secret keys and the public messages, together with any $t-1$ shadows, provides no information about the new secret.

Lemma 5. *For $L \geq i \geq 0$,*

$$I(K_i; K_0, K_1, ..., K_{i-1}, \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) = 0 \qquad \text{if } k \leq t-1. \quad (9)$$

Proof. Recall from information theory that conditional mutual information is defined as $I(X;Y|Z) = H(X|Z) - H(X|Y,Z) = H(Y|Z) - H(Y|X,Z)$ and satisfies the identity $I(X,Y;Z) = I(X;Z) + I(Y;Z|X)$. Thus,

$$\begin{aligned} & I(K_i; K_0, K_1, ..., K_{i-1}, \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) \\ = & I(K_i; \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) \\ & + I(K_i; K_0, ..., K_{i-1} | \Delta_i(k), P_1, ..., P_i, S_1, ..., S_i). \end{aligned}$$

If we can show that $I(K_i; K_0, ..., K_{i-1}|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) = 0$ when $k \leq t-1$, then (9) follows directly from (8). But

$$I(K_i; K_0, ..., K_{i-1}|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) \leq H(K_i|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i)$$

and $H(K_i|\Delta_i(k), P_1, ..., P_i, S_1, ..., S_i) = 0$ by (4), so the desired result follows. □

We next observe the following identiy.

Lemma 6. *For $j \geq i+1$,*

$$I(K_i; S_j|\Delta_i(t-1), P_1, ..., P_i, K_0, .., K_{i-1}) = m.$$

Proof.

$$\begin{aligned} & I(K_i; S_j|\Delta_i(t-1), P_1, ..., P_i, K_0, ..., K_{i-1}) \\ = \; & I(K_i; S_j, \Delta_i(t-1), P_1, ..., P_i, K_0, .., K_{i-1}) \\ & -I(K_i; \Delta_i(t-1), P_1, ..., P_i, K_0, .., K_{i-1}) \\ = \; & I(K_i; \Delta_i(t), P_1, ..., P_i, K_0, ..., K_{i-1}) \\ = m. & \end{aligned}$$

The second equality is obtained because $j \geq i+1$ and thus joining S_j with $\Delta_i(t-1)$ gives a set $\Delta_i(t)$ for use in (7), and by noticing that the second term in the previous equation is 0 from Lemma 5 because mutual information is nonnegative and $I(X;Y) \leq I(X;Y,Z)$. The last equality is obtained directly from Lemma 5. □

Proof of theorem. We first observe that for $j = 1, ..., n$, we may choose $S_j = S_{L+1}$. Thus $H(S_j) = H(S_{L+1})$ and we need to show only that $H(S_{L+1}) \geq (L+1)m$. Now,

$$\begin{aligned} & H(S_{L+1}) \\ & \geq H(S_{L+1}|\Delta_L(t-1)) \\ & \geq H(S_{L+1}|\Delta_L(t-1)) - H(S_{L+1}|P_1, ..., P_L, K_0, .., K_L, \Delta_L(t-1)) \\ & = I(P_1, ..., P_L, K_0, ..., K_L; S_{L+1}|\Delta_L(t-1)). \end{aligned}$$

If we can show that the last quantity is at least $(L+1)m$, then the theorem is proved. But

$$\begin{aligned} & I(P_1, ..., P_L, K_0, ..., K_L; S_{L+1}|\Delta_L(t-1)) \\ & = \sum_{i=1}^{L} I(P_i; S_{L+1}|\Delta_L(t-1), P_1, ..., P_{i-1}) \\ & \qquad + \sum_{i=0}^{L} I(K_i; S_{L+1}|\Delta_L(t-1), P_1, ..., P_i, K_0, ..., K_{i-1}) \\ & \geq \sum_{i=0}^{L} I(K_i; S_{L+1}|\Delta_L(t-1), P_1, ..., P_i, K_0, ..., K_{i-1}) \\ & = (L+1)m \end{aligned}$$

where the last equality is obtained directly from Lemma 6. □

We have shown that if a (t, n) threshold scheme can disenroll L participants, then each secret shadow must contain at least $(L+1)H(K_0)$ bits. In the next section we exhibit three examples of such threshold schemes where each shadow contains exactly $(L+1)H(K_0)$ bits.

3 Threshold Schemes with Disenrollment Capability

In this section we will exhibit three examples of perfect (n, t) threshold schemes that allow disenrollments and achieve the lower bound on shadow size established in the previous section

3.1 Brickell-Stinson Scheme[2]

Let $(K, S_1, ..., S_n)$ be a perfect (n, t) threshold scheme, where K represents the secret chosen from $\mathbb{K}$ and S_i represents a shadow chosen from $\mathbf{S}$. We further assume that $H(K) = m$. An (n, t) threshold scheme with L-fold disenrollment capability $(K_0, ..., K_L, \tilde{S}_1, ..., \tilde{S}_n, P_1, ..., P_L)$ can be constructed from $(K, S_1, ..., S_n)$ as follows:

- Each K_i represents a secret chosen uniformly from $\mathbb{K}$.

- Each $\tilde{S}_i$ represents a shadow $\tilde{S}_i = (S_i, R_{i,1}, ..., R_{i,L})$ where each $R_{i,j}$ is a random binary string of length m.
- When $\tilde{S}_i$ is invalidated, a new key K_i is chosen and associated with it are the new shadows $\{S^i_{i+1}, ..., S^i_n\}$ that are formed as specified by the original (n,t) threshold scheme. The public message P_i that is broadcast through the public channel is the union of messages of the type

$$\{R_{i+1,i} + S^i_{i+1}, R_{i+2,i} + S^i_{i+2}, ..., R_{n,i} + S^i_n\}.$$

Note that each $R_{i,j}$ is a random string and can be considered as a one-time pad that protects the shadow S^i_j; thus, $H(S^i_j) = H(S^i_j|P_i)$ and $H(K_i) = H(K_i|\Delta_i(k), P_1, ..., P_i)$ for $k < t$. Furthermore, it is easy to check that each shadow contains $(L+1)m$ bits which is the lower bound given in Section 2. So, we have the following theorem.

Theorem 7. *The Brickell-Stinson scheme is a perfect (n,t) threshold scheme with L-fold disenrollment capability that achieves the lower bound, $H(S_j) = (L+1)m$.*

3.2 Nonrigid Hyperplane Scheme

For simplicity we first consider the case where $L = t - 1$; the cases where $L \neq t - 1$ can be similarly designed and will be discussed later. Let $\mathbb{H}$ be the collection of all hyperplanes in a t-dimensional vector space E over $GF(q)$. The n hyperplanes represented by the rows of an n by $t+1$ augmented matrix

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,t-1} & 1 & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,t-1} & 1 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,t-1} & 1 & b_n \end{bmatrix} \tag{10}$$

must be in general orientation, that is, the unaugmented n by t matrix

$$U(A) = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,t-1} & 1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,t-1} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,t-1} & 1 \end{bmatrix} \tag{11}$$

must have the property that every one of its t by t submatrices is nonsingular. The intersection of the hyperplanes corresponding to any t or more rows of this matrix is a point v, whose first coordinate is the secret K_0. The intersection of hyperplanes corresponding to any collection of fewer than t rows must intersect in an affine subspace consisting of points which do not all share a common first coordinate. Equivalently, the vector (10...0) must never appear as a row in the row reduced echelon form of any j by t submatrix of $U(A)$ given in (11) if $j < t$.

Let K_i correspond to the first coordinate of an arbitrarily chosen point v_i in the vector space E. Corresponds to every point v' in E, there is a translation of hyperplanes such that the new point of intersection is the point v'. Each shadow S_j is given by the j-th row of the matrix A in (10). Clearly, every shadow consists of $t \log_2 q$ bits, which is the lower bound given in Section 2. On revealing S_j, the public information P_j is the collection of translations of the unrevealed hyperplanes, that is, $\{c_{j,j+1}, c_{j,j+2}, ..., c_{j,n}\}$ such that the i-th newly translated hyperplane can be easily computed by converting the last entry in A to $b_i + c_{j,i}$.

Theorem 8. *The nonrigid hyperplane scheme is a perfect (n,t) threshold scheme with t-fold disenrollment capability that achieves the lower bound, $H(S_j) = t \log_2 q$.*

Proof. To show that the hyperplane scheme is a perfect (n,t) threshold scheme, we need to show that every key in $\mathbb{K}$ remains equally probable after each disenrollment. Let ℓ be a 1-dimensional subspace in E determined by $t-1$ hyperplanes in $\Delta_i(t-1)$, and let $\{v_0, \ldots, v_{i-1}\}$ be the chosen points in E that correspond to the known secrets $K_0, \ldots, K_{i-1}$ as defined above. For each each $j > i$, the translations of these chosen points given by $V = \{v_0, v_1 - (0, \ldots, c_{1,j}), \ldots, v_{i-1} - (0, \ldots, c_{i-1,j})\}$ must be contained in the hyperplane corresponding to participant j. Since $i \leq t-1$, for every point $p \in \ell$ and every $j > i$, there exists a hyperplane $H_j \in \mathbb{H}$ that contains the point p and the corresponding translated points in V. In other words, every $p \in \ell$ can be the chosen point v_i and every key can be the new secret. Thus, the entropy of every key remains the same and (6) is established. □

In the case where the number of disenrollment L is less than $t-1$, we publish $t-1-L$ columns of the matrix $U(A)$ in (11) and still maintain the same perfect threshold scheme properties. If L is greater than $t-1$, then we use the additional columns to store informations about changing the orientation of each of the hyperplane after each disenrollment. Consider $L = t + x, x \geq 0$ and the matrix in (10) representing the shadows is then given by

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,t+x} & 1 & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,t+x} & 1 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,t+x} & 1 & b_n \end{bmatrix} \tag{12}$$

After i disenrollments, each new hyperplane is then given by $(a_{j,i_0}, \ldots, a_{j,i_{t-2}}, 1, b_j + c_{i,j})$ where $i_m = 1 + (i + m \bmod t + x)$ and $c_{i,j}$ isthe corresponding broadcast translation. Such a scheme can be shown to be perfect by using similar arguments as above.

3.3 Martin Scheme[5]

Every $(n, t+i)$ threshold scheme, $i \geq 0$, can be used as an (n,t) threshold scheme by publishing i additional shadows from the shadow space $\mathbf{S}$. Thus, any t or more shadows together with the i published shadows can uniquely determine the secret. Based on the above notion, an (n,t) threshold scheme with L-fold disenrollment capability $(K_0, \ldots, K_L, \tilde{S}_1, \ldots, \tilde{S}_n, P_1, \ldots, P_L)$ can be constructed from $L+1$ randomly chosen perfect $(n, t+L)$ threshold schemes $(K_i, S_1^i, \ldots, S_n^i), i = 0, \ldots, L$ as follows:

- Each K_i represents a secret chosen from the key space, $\mathbb{K}$.
- Each $\tilde{S}_i$ represents a shadow of the form $(S_i^0, S_i^1, \ldots, S_i^L)$ where each S_i^j is a shadow from the j-th $(n, t+L)$ threshold scheme, $(K_j, S_1^j, \ldots, S_n^j)$.
- When $\tilde{S}_i$ is invalidated, the new key K_i is used and associated with it, L additional "new" shadows have to be published. Among these L additional shadows are the revealed shadows, $S_1^i, S_2^i, \ldots, S_i^i$.

Since all the $L+1$ keys, $K_0, K_1, \ldots, K_L$, are independent of one another, the disclosures of K_j and $S_\ell^j, \ell \geq 1$, give no information on K_i, as long as $i \neq j$. However, the disclosed shadows, $S_1^i, \ldots, S_i^i$, together with $L+t-i$ other shadows can uniquely determine the key K_i. Thus, only $L-i$ additional shadows from $\mathbb{S}$ are needed to be broadcast through the public channel, and we have the following theorem,

Theorem 9. *The Martin scheme is a perfect (n,t) threshold scheme with L-fold disenrollment capability that achieves the lower bound, $H(\tilde{S}_i) = (L+1)H(K_i)$.*

We can further modify the Martin Scheme to reduce the size of the public broadcast after each disenrollment. Specifically, we randomly choose an $(n, t+i)$ threshold scheme (instead of an (n, t_L) threshold scheme), for $0 \leq i \leq L$. After the i-th disenrollment, we use the i revealed shadows $S_1^i, \ldots, S_i^i$ as the additional shadows required to be published, thus reducing the size of the broadcast message.

4 Conclusion

We have established a lower bound on the initial overhead required for (n,t) threshold schemes that allow disenrollments and have given three examples of such implementations. We further modify the Martin Scheme to reduce the cost of broadcasting the public informations. An interesting open question remained to be solved is "What is the lower bound on the entropy of the public broadcast". We conjecture that the lower bound is given by

Conjecture. For $0 \leq i \leq L$,

$$H(P_i) \geq iH(K).$$

References

1. G.R. Blakley, *Safeguarding Cryptographic Keys.* Proceedings AFIPS 1979 Nat. Computer Conf. **48** (1979) 313–317
2. E.G. Brickell and D.R. Stinson, *oral communication.*

3. M. De Soete and K. Vedder, *Some New Classes of Geometric Threshold Schemes*, Proceedings EUROCRYPT 88 (1988).
4. E.D. Karnin, J.W. Greene and M.E. Hellman, *On Secret Sharing Systems*, IEEE Trans. on Information Theory, **IT-29** (1983), 35–41
5. K.M. Martin, *Untrustworthy Participants in Perfect Secret Sharing Schemes*, preprint
6. R.J. McEliece and D.V. Sarwarte, *On Sharing Secrets and Reed-Solomon Codes*, Communications of ACM **24** (Sept 1981), 583–584
7. A. Shamir, *How to Share a Secret*, Communications ACM **22** (Nov 1979), 612–613
8. C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal (1948), 656–715
9. D.R. Stinson and S.A. Vanstone, *A Combinatorial Approach to Threshold Schemes*, SIAM J. Disc. Math. **1–2** (1988), 230–236