GENERALIZED LINEAR THRESHOLD SCHEME

S.C. Kothari
Department of Computer Science
Iowa State University
Ames, Iowa 50011

ABSTRACT

A generalized linear threshold scheme is introduced. The new scheme generalizes the existing linear threshold schemes. The basic principles involved in the construction of linear threshold schemes are laid out and the relationships between the existing schemes are completely established. The generalized linear scheme is used to provide a hierarchical threshold scheme which allows multiple thresholds necessary in a hierarchical environment.

INTRODUCTION:

The protection of important information is an age old problem. In any scheme devised to protect information, care has to be taken to ensure that the information does not get lost, destroyed, or into wrong hands, and at the same time the scheme should be efficient. A simple solution to protect the information from loss or destruction, is to make multiple copies of the information and distribute the copies. But with multiple copies the probability that the information will get into wrong hands, increases and the simple solution becomes unacceptable. The question of protection of information has received a lot of attention in recent years because of the proliferation of computers into areas such as electronic mail, electronic fund transfer, and storage of information.

There have been several schemes, called cryptosystems, developed in the past to protect information. A very important and interesting class of cryptosystems called the public key cryptosystems came into existence in the seventies. The important concept underlying the public key cryptosystems is to create a cryptosystem such that the knowledge of the encoding key does not lead to the computation of the decoding key in a reasonable amount of computer time. This enables the public key cryptosystems to make the encoding key public and also solve the problem of electronic signature. The reader is referred to [Diffie 76], [Rivest 78] for discussion of the public key cryptosystems. In 1979, a different type of protection scheme, called the threshold scheme[1] was introduced independently by Blakely and Shamir. The important idea underlying the threshold scheme is to create "shadows"[2] of the message (secret) such that

[1] The other commonly used names for threshold schemes are key safeguarding schemes and secret sharing schemes.

[2] The term "shadows" was originally introduced by Professor Blakely in [Blakely 79].

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 231-241, 1985.

unless a certain number (called the threshold) of "shadows" are not available the message (secret) cannot be retrieved. Discussion of the threshold schemes is found in [Blakely 79], [Shamir 79]. Several other threshold schemes have been introduced since then.

This paper focuses on four of the existing threshold schemes [Blakely 79], [Shamir 79], [Bloom], [Karnin 83]. It is shown that the four schemes are founded on common principles derived from linear algebra and for this reason we will refer to these four schemes as linear threshold schemes. A generalized linear threshold scheme which subsumes the various threshold schemes is presented. The generalized threshold scheme extracts the essence of the linear threshold schemes, making transparent the basic principles.

Roughly speaking a generalized linear threshold scheme works as follows. A secret is represented by a scalar and a linear variety is chosen to conceal the secret. A linear functional fixed in the beginning, and known to all trustees is used to reveal the secret from the linear variety. The n shadows are hyperplanes containing the linear variety. Moreover the hyperplanes are chosen to satisfy the condition that the intersection of less than t ($t \leq n$) of them results in a linear variety which projects uniformly over the scalar field by the linear functional used for revealing the secret. The number t is called the threshold. Thus as more shadows are known more information is revealed about the linear variety used to keep the secret, however, no information is revealed until the threshold number of shadows are known.

Karnin et al show in [Karnin 83] that Shamir's, and Blakeley's schemes are special cases of their threshold scheme. It is shown here that with the exception of Shamir's scheme the remaining three threshold schemes are equivalent to each other and explicit algorithms are presented to convert one scheme to another. The Shamir's scheme is a specialization of the remaining three schemes and all the four schemes are specializations of the generalized linear threshold scheme. Also a much simpler proof of perfect security compared to [Blakely 81] is presented. This proof nicely explains the common mechanism used for perfect security in various linear threshold schemes.

The generalized linear threshold scheme allows linear varieties of positive dimension to conceal the secret. This fact is utilized in constructing a hierarchical threshold scheme. The hierarchical threshold scheme uses a chain of linear varieties to keep a secret and allows multiple thresholds for hierarchy of trustees.

2. DEFINITIONS AND PRELIMINARY RESULTS

In this section some preliminary results and definitions are discussed. This material will be used in the construction of the generalized threshold scheme and also in the proofs to show that other threshold schemes are specializations of the generalized threshold scheme. Some of these are standard results but they are included here for the sake of completeness and to fix the notation. The interested readers may look at [Kuiper 65] for further discussion.

DEFINITION: A threshold scheme is a process which coverts a given number x called the "message" to n other numbers y_i's called the "shadows" which satisfy the property: there exists a number t ($t \leq n$) called the threshold such that x can be retrieved if any t of the n "shadows" are known, but less than t "shadows" reveal no information about the message. More specifically such a threshold scheme is called t out of n threshold scheme.

Using the entropy function H from [Shannon 48] we can state the requirements in the threshold scheme as

(i) $H(x \mid y_{i_1}, y_{i_2},..y_{i_t}) = 0$

(ii) $H(x) = H(x \mid y_{i_1},y_{i_2},..y_{i_{t-1}})$

for an arbitrary set of t indices $\{i_1,i_2,..,i_t\}$.

Let k denote a finite field and k^n denote the set consisting of n-tuples over k. The set k^n is a vector space over k of dimension n in a natural way. The set k^n is also called an affine space over k and the individual n-tuples are referred to as the points of the affine space.

DEFINITION: A subset S of k^n is called an affine variety of k^n if there exist a finite set $f_i(x_1,x_2,...,x_n)$, i = 1,2,..,m, of polynomials in n variables such that

$S = \{(a_1,a_2,..,a_n) \in k^n \mid f_i(a_1,a_2,..a_n)=0 \text{ for } i=1,2,..,m.\}$

The equations $f_i(x_1,x_2,..,x_n) = 0$ are called the defining equations of the affine variety S.

DEFINITION: An affine variety is called a linear variety if all its defining equations are linear.

DEFINITION: A linear variety is called a homogenous linear variety if all its defining equations are homogeneous.

Given a linear polynomial $f(x_1,x_2,..x_n) = b_0+b_1x_1+b_2x_2+..+b_nx_n$, we represent it by the vector $(b_0,b_1,..b_n)$ in k^{n+1}, representing the coefficients of f. We will identify a linear polynomial $f(x_1,x_2,..,x_n)$ with the vector representing its coefficients.

DEFINITION: Given a linear variety S, define

$E(S) = \{f \in k^{n+1} \mid f(a_1,a_2,..,a_n)=0 \text{ for all } (a_1,a_2,..,a_n) \in S\}$.

E(S) is a vector subspace of k^{n+1}.

DEFINITION: Given subsets S and W of k^n and vector c in k^n define $S = c+W$ if

$S = \{v \in k^n \mid v = c+w \text{ for } w \in W\}$.

The function dim( ) is used to denote the dimension of a vector space.

LEMMA 1: Given a linear variety S of k^n, there exists a vector $c = (c_1, c_2, .. c_n)$ and a vector subspace W of k^n such that

(i) $S = c + W$

and

(ii) $\dim(W) + \dim(E(S)) = n$.

Proof: The proof follows from the Gaussian elimination process and other standard arguments from vector space theory.

DEFINITION: For a linear variety $S = c+W$, define dim(S) to be dim(W).

NOTATION: Given a linear variety S, the notation $S = w + W$ indicates that w is a vector and W is a vector subspace of k^n.

LEMMA 2: Let $S_1 = w_1+W_1$, and $S_2 = w_2+W_2$ be linear varieties of k^n. Then $S_1 \cap S_2$, is either empty or else it is a linear variety such that $S_1 \cap S_2 = w + W$ where W contains $W_1 \cap W_2$.

Proof: The proof follows from standard vector space arguments.

DEFINITION: Given vector subspaces W_1 and W_2 of k^n, $W_1 + W_2$ is defined as the vector space where

$$W_1 + W_2 = \{v \in k^n \mid v = w_1+w_2 \text{ for } w_i \in W_i \text{ for } i=1,2.\}$$

The following is a standard result from the vector space theory.

LEMMA 3: If W_1 and W_2 are vector spaces of k^n then

$$\dim(W_1+W_2) = \dim(W_1)+\dim(W_2)-\dim(W_1 \cap W_2).$$

DEFINITION: If S is a linear variety of k^n such that $\dim(E(S)) = 1$ then S is called a hyper plane.

LEMMA 4: Let $S=w+W$ be a linear variety and $t = \dim(E(S))$. Let $H_1, H_2, .., H_m$ be hyperplanes containing S. Then,

(i) If $m < t$ then $\bigcap_{i=1}^{m} H_i$ strictly contains S,

(ii) If $\bigcap_{i=1}^{m} H_i = S$ then $m \geq t$.

Proof: Note that (ii) clearly follows from (i) because H_i contains S for i-1,2,..,m. Let $T = \bigcap_{i=1}^{m} H_i$. Clearly $E(T) = E(H_1)+E(H_2)+...+E(H_m)$. By repeated applications of

Lemma 3 it follows that $\dim(E(T)) \leq m$. If $m < t$ then it follows from Lemma 1 that $\dim(S) < \dim(T)$, thus T strictly contains S.

DEFINITION: Let S be a linear variety and $t = \dim(E(S))$. The hyperplanes $H_1, H_2, .., H_m$ for $m \geq t$, are said to be in general position with respect to S, if the intersection of any t of them is S.

DUALIZATION PRINCIPLE: Let V be a vector space of dimension n over the base field k. Let $\widetilde{V}$ be the set of linear functionals on V then $\widetilde{V}$ itself forms a vector space of dimension n called the dual space of V. The space $\widehat{V}$ can be identified with k^n as follows:
Fix a basis of V. Then for every linear functional L on V there exist a unique vector $(a_1, a_2, .., a_n)$ in k^n such that for every v in V,

$$L(v) = a_1v_1 + a_2v_2 + \ldots + a_nv_n,$$

where $(v_2, v_2, .., v_n)$ is the representation of v with respect to the fixed basis of V. For every L belonging to the dual space $\widehat{V}$ we identify it with the vector $(a_1, a_2, .., a_n)$ in k^n as described above.

DEFINITION: Given a vector v belonging to a vector space V and an element a of k, define

$$H(v,a) = \{L \in \widetilde{V} \mid L(v)=a\}.$$

LEMMA 5: Given a vector v in V and an element a in k the set H(v,a) is a hyperplane in $\widehat{V}$.

Proof: Let $v=(v_1, v_2, .., v_n)$ be the representation of v with respect to a fixed basis of V. Then by the dualization principle H(v,a) can be identified with the set

$$\{(a_1, a_2, .. a_n) \in k^n \mid a_1v_1 + a_2v_2 + .. + a_nv_n = a\}$$

Thus E(H(v,a)) is a vector space of dimension one, generated by the vector $(-a, v_1, v_2, .., v_n)$ and so H(v,a) is a hyperplane.

LEMMA 6: Let V be a vector space of dimension n. Let v_i for $i=1,2,..,m, m \geq n$, be vectors in V such that any n of them are linearly independent. Let L be a linear functional on V and let $L(v_i)=a_i$ for $i=1,2,..,m$. Then the hyperplanes $H_i=H(v_i, a_i)$ are in general position with respect to (L).

Proof: Since $L(v_i) = a_i$, L belongs to H_i for $i=1,2,..,m$. By lemma 1, $\dim(E(\{L\}))=n$. For $i=1,2,..,m$, by (v_i, a_i) we denote the vector in k^{n+1} whose projection on the first

n components is given by the vector v_i and the (n+1)-th component is a_i. Any of the n vectors (v_i,a_i) for i=1,2,..,m are linearly independent because the same property is true for their projections v_i's by assumption. To prove that the hyperpland H_i are in general position we need to show that intersection of any n of them is {L}.

Let $S = \bigcap_{i=1}^{n} H_i$. Without loss of generality it is enough to show that S = {L}.

By lemma 2, S is a linear variety. L belongs to S because L belongs to every hyperplane H_i for i=1,2,..,m. The vectors (v_i,a_i) belong to E(S) for i=1,2,..,n. Since the vectors are linearly independent it follows that dim(E(S))=n. Then by lemma 1, dim (S) = 0 and so S = {L} since L belongs to S.

LEMMA 7: Let $v_i=(1,b_i,b_i^2,\ldots,b_i^{n-1})$ be vectors belonging to k^n for i=1,..,m where $m \geq n$ and $b_i \neq b_j$ for $i \neq j$ then any n of the m vectors v_i's are linearly independent.

Proof: Without loss of generality it is enough to show that v_i's for i=1,2,...,n are linearly independent. Let B be the n x n matrix such that its (i,j)-th entry is b_i^{j-1}. The matrix B is known as a Vandermonde matrix. It is a property of a Vendermonde matrix that [3] $\det(B) \neq 0$ if and only if $b_i \neq b_j$ for $i \neq j$. Thus if $b_i \neq b_j$ for $i \neq j$ then $\det(B) \neq 0$ which implies that v_i's are linearly independent for i=1,2,..,n.

Definition: Given a linear functional f and an element a belonging to k define $H(f,a) = \{v \in V \mid f(V) = a\}$.

LEMMA 8: H(f,a) is a hyperplane in V.

Proof: This is a dual of lemma 5.

The following lemma is the mathematical basis for the perfect security of the various linear threshold schemes.

LEMMA 9: Let f be a linear functional on a vectorspace V. T is a linear subvariety of V such that T is not contained in H(f,a) for any a belonging to k. Then f uniformly projects T over k.

Proof: Since T is not contained in any H(f,a), f projects T onto k.

Let $T_a = \{V \mid v \in T \text{ and } f(v) = a\}$. Then $T_a = v_a + W$ where v_a is a vector in T which projects to a and W is subspace contained in the kernel of f and it does not depend on a. Thus cardinality of T_a which is the same as the cardinality of W is independent of a i.e. f projects T unifromly over k.

3. DESCRIPTION OF LINEAR THRESHOLD SCHEMES

In this section we briefly describe the threshold schemes due to Blakely, Bloom, Karnin-Greene-Hellman and Shamir. For more detailed descriptions of these schemes refer to [Blakely 79], [Shamir 79], [Bloom], [Karnin 83]. For uniformity of descriptions all the three schemes are set up to give n "shadows" and the threshold is t where n and t are integers such that $n \geq t$.

Blakely's Threshold Scheme (affine version):

Blakely's threshold scheme starts with a t dimensional affine space V. The key is concealed by specific coordinate of a point S of V. The n "shadows" are given by hyperplanes H_i, i=1,2,..,n, of V such that the H_i and the specific coordinate plane passing through S are in general position with respect to S.

Now given any t distant "shadows" H_i, we can get the point S representing the key by intersecting the "shadows". However if only r "shadows", $r < t$, are known, then by intersecting the r hyperplanes corresponding to the "shadows" we get (t-r) dimensional linear variety strictly containing S. Thus S cannot be determined and no information about the key is revealed.

Bloom's Threshold Scheme:

Bloom's scheme starts with a t dimensional vector space V. The n vectors v_i for i=0,1.,,n, are chosen such that any t of them are linearly independent and consequently span the vector space C. A linear functional L on V is chosen such that $L(v_0)$ represents the key. The "shadows" S_i for i=1,2,..,n are defined to be $S_i=L(v_i)$. Now, given any t the linear functional L is completely determined and the key can be computed using v_0. However if any r "shadows", $r < t$, are known then L is not completely determined and no information about the key is revealed.

Shamir's Threshold Scheme:

Shamir's scheme starts with a polynomial

$$f(x) = a_0+a_1x+a_2x^2+..+a_{t-1}x^{t-1},$$

and nonzero distinct scalars b_i for i=1,2,..n. The key S is represented by a_0. The n "shadows" S_i, for i=1,2,..n are defined as

$$S_i = f(b_i) .$$

Given any t distinct "shadows" f(x) can be determined by Lagrange interpolation formula and the key is obtained by evaluating f(x) at x=0. If only r "shadows", $r < t$, are known then f(x) cannot be determined and no information about the key is revealed.

Karnin-Greene-Hellman Threshold Scheme:

The scheme starts with n+1 column vectors $A_0,A_1,..,A_n$ of size t such that any t

of them have full rank. U is a row vector of size t. The key is given by $U \cdot A_0$. The n shadows are given by $U \cdot A_i$ for i=1,2,..,n. If any t of the n shadows are known then U can be determined and the key is obtained by evaluating $U \cdot A_0$. If less than t shadows are known then U is not determined and no information about the key is revealed.

4. GENERALIZED LINEAR THRESHOLD SCHEME:

A generalized t out of n threshold scheme is constructed as follows. Let V be a (d+t) dimensional vectorspace. The secret is a scalar α concealed by a d dimensional linear subvariety S. A linear functional f is used to reveal the secret from S i.e. f is chosen such that f(v) is equal to α for any v belonging to S. The linear variety S is kept secret but the linear functional f is made known to all the trustees involved.

The n shadows are given by n hyperplanes. The hyperplanes representing the shadows and the hyperplane $H(f,\alpha)$ together are chosen to be in general position with respect to S.

Given any t shadows, S is obtained by intersecting the corresponding hyperplanes. If less than ($< t$) shadows are known the corresponding hyperplanes intersect in a linear subvariety S' containing S. Moreover S' is not contained in $H(f,\alpha)$ because the hyperplanes intersecting in S' and $H(f,\alpha)$ are in general position by choice. In view of lemma 9 S' reveals no information about α.

5. INTERRELATION OF LINEAR THRESHOLD SCHEMES:

This section presents conversion algorithms proving that the t out of n threshold schemes of Blakely, Bloom and Karnin-Greene-Hellman are equivalent. The same notation that is used to describe the schemes is used again to describe the algorithms.

Algorithm BLBM:

The following algorithm converts a Blakely scheme to a Bloom scheme.

1. Let $e_1, e_2, .., e_t$ be the standard basis of V.
   Choose the linear functional L such that $L(e_i)$ is the i-th coordinate of S for $1 \leq i \leq t$.
2. If the k-th coordinate of S is the secret to be concealed then choose v_0 to be e_k.
3. Choose v_i to be the vector representing the coefficients of H_i for i=1,2,..,n.

Algorithm BMKGH:

The following algorithm converts a Bloom scheme to a Karnin-Greene-Hellman scheme.

1. Let $e_1, e_2, .., e_t$ be the standard basis of V. Set $U = (L(e_1), L(e_3), .., L(e_t))$.

2. The (n+1) column vectors are chosen to be $v_0, v_1, .., v_n$ written as column vectors.

Algorithm KGHBL:

The following algorithm converts a Karnin-Greene-Hellman scheme to a Blakely scheme.

1. Choose S to be the point given by U.
2. The hyperplanes $H_1, H_2, .., H_n$ are chosen to be the hyperplanes whose coefficient vectors are given by $V_1, V_2, .., V_n$.

Algorithm BMSH:

This algorithm converts a Bloom's scheme to a Shamir's scheme.

1. Define $v_0 = (1,0,..,0)$
2. Define the vectors v_i for $1 \leq i \leq n$ as
   $v_i = (1, b_i, b_i^2, .., b_i^{t-1})$.
   Note that by lemma 7 any t of the v_i's for i=0,2,..,n are linearly independent.
3. Let $a = (a_0, a_1, .., a_{t-1})$ and define L as,
   $L(v) = a \cdot v$ for v belonging to v, where $a \cdot v$ is the dot product of a and v.

Algorithm GSBL:

This algorithm specializes a generalized linear scheme to a Blakely scheme.

1. Choose d = 0.
2. Choose the linear functional f to be a projection on one of the coordinate axis.

In view of these algorithms the various threshold schemes are specializations of the Generalized linear threshold scheme and they subsume Shamir's scheme.

6. HIERARCHICAL THRESHOLD SCHEME:

In many applications there is a hierarchy among the trustees to whom the shadows are distributed for safeguarding the secret, and there is a need to create shadows of different potency. For example in a company where there are two levels of guards like senior and junior executives, it may be required that the threshold to obtain the secret be strictly smaller for senior executives compared to the threshold required of junior executives. In defense applications, this requirement may be even more crucial when there are different levels of commands and it is required that the lower

the level of command the higher the number of officers required to reveal the secret. These applications require a threshold scheme which provides shadows at different levels and the threshold is dependent on the level, such a scheme will be called a hierarchical threshold scheme.

An obvious solution to obtain a hierarchical threshold scheme seems to be to adopt an ordinary threshold scheme to the purpose by providing multiple shadows as shadows at higher levels. However this approach has drawbacks such as even though less shadows are required to reveal the secret the computation required in the process is not reduced, the shadows at different levels have to be physically different and interpreted differently, and a full range of threshold values is not available. A natural solution to these problems is offered by a generalized linear scheme.

A hierarchical threshold scheme is obtained from generalized linear threshold scheme as follows. The basic idea is to use linear varieties of different dimensions to conceal the secrets, at different levels.

Assume that V is a t dimensional vector space and f is a linear functional which is used to reveal the secret concealed by a linear subvariety S. The variety S is such that function f has a unique value, on S. There are several choices for S and the maximum dimension for S is (t-1). The threshold is the difference between t and the dimension of S. Choose a sequence S_l, $0 \leq l \leq t-1$, of linear subvarieties such that $\dim(S_i) = i$ and $f(S_i)$ is a single value giving the secret. The shadows at level i are generated with respect to S_i as described in the construction of generalized linear threshold scheme. The threshold at level i is then t-i. Thus we get a hierarchical scheme providing t different levels of shadows. At level i, t-i linear equations have to be solved to obtain the secret, thus the computation to reveal the secret is proportional to the threshold.

7. CONCLUSIONS

This paper shows that various linear threshold schemes are closely related and they are all founded on the same principles. A generalized linear threshold scheme nicely crystalizes the basic principles of linear threshold schemes. The generalized threshold scheme has the flexibility which allows a chain of linear varieties to be used to conceal a secret. This property provides a hierarchical threshold scheme. The linear threshold schemes have fallen back on Shamir's method for a concrete implementation - however the same method cannot be used to implement a generalized threshold scheme as a hierarchical scheme. At this time we do not know of any efficient implementation of a hierarchical threshold scheme and the problem needs to be investigated further.

There are other possible generalizations of linear threshold schemes. The linear functional used to reveal the secret may be replaced by a fractional linear transformation (this is the case with Blakeley's projective threshold scheme) also the shadows may be chosen to be lower dimensional linear varieties instead of linear

hyperplanes. It is not clear that these generalizations would give any better threshold schemes.

ACKNOWLEDGEMENTS:

I thank Professor Blakely for the stimulating and valuable discussions on the subject of this paper. I thank Dr. Lakshmivarahan for initiating my interest in the subject. I thank Dr. Robert Roberts for suggesting some improvements in the manuscript.

REFERENCES:

[Blakely 79] Blakely G.R., "Safeguarding Cryptographic Keys", Proceeding of the National Computer Conference, 1979, AFIPS Conference Proceedings, Vol. 48 (1979), pp. 313-317.

[Blakely 81] Blakely G.R. and Laif Swanson, "Security Proofs for Information Protection Systems", Proceedings of the 1981 symposium on Security and Privacy, IEEE Computer Society, 1981, pp. 75-88.

[Bloom 81] Bloom J.R., "A Note on Superfast Threshold Schemes", Preprint Texas A&M University, Department of Mathematics (1981).

[Diffie 76] Diffie W. and Hellman, M.E., "New Directions in Cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, No. 6, November 1976, pp. 644-654.

[Karnin 83] Karnin, Greene and Hellman, "On Secret Sharing Systems", IEEE Transactions on Information Theory, Vol. IT-29, (1983), pp. 35-41.

[Kuiper 65] Kuiper, "Linear Algebra and Geometry", North-Holland Publishing Company-Amsterdam, Second Edition, 1965.

[Rivest 78] Rivest R.L., A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, Vol. 21, 1978, pp. 120-126.

[Shamir 79] Shamir A., "How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, Nov. 1979, pp. 612-613.

[Shannon] Shannon C.E., "Communication Theory of Secrecy Systems", Bell System Technical Journal, 1948, pp. 656-715.