

Threshold Schemes

An important cipher key K must be protected from (a) accidental or malicious exposure (causing vulnerability) and (b) loss or destruction (causing inaccessibility).

Both problems may be alleviated by the use of shadows in a threshold scheme.

A (t, w) *threshold scheme* is a system of protecting a key K by breaking it into w *shadows* (pieces) K_1, \dots, K_w in such a way that (a) it is easy to compute K using knowledge of any t of the shadows K_i , but (b) it is impossible to compute K because of lack of information if one knows any $t - 1$ or fewer of the shadows K_i .

The w shadows are given to w users. Since (at least) t shadows are needed to find K , no group of fewer than t users can conspire to get the key.

At the same time, if a shadow is lost or destroyed, one can still compute K so long as at least t valid shadows remain.

Lagrange Interpolating Polynomial Threshold Scheme

A. Shamir proposed a (t, w) threshold scheme based on Lagrange interpolating polynomials.

A polynomial of degree $t - 1$ is determined by its values at t distinct values of its argument.

The shadows come from a random polynomial of degree $t - 1$:

$$h(x) = (a_{t-1}x^{t-1} + \cdots + a_1x + a_0) \bmod p$$

with constant term $a_0 = K$.

All arithmetic is done modulo p , where p is a prime number greater than both K and w . Long keys can be broken into smaller blocks to avoid computing modulo a large prime.

Given $h(x)$, the key K is easily computed by $K = h(0)$.

The w shadows are defined as the value of $h(x)$ at w distinct points. For example, one might let $K_i = h(i)$ for $1 \leq i \leq w$.

Given t shadows K_{i_1}, \dots, K_{i_t} , one may construct $h(x)$ as a Lagrange polynomial

$$h(x) = \sum_{s=1}^t K_{i_s} \prod_{\substack{j=1 \\ j \neq s}}^t \frac{(x - i_j)}{(i_s - i_j)} \bmod p.$$