Example of the LIP Threshold Scheme

Let \( t = 3, \ w = 5, \ p = 13, \ K = 10 \) and
\[
h(x) = (6x^2 + 7x + 10) \mod 13
\]
with random coefficients 6 and 7.

The five shadows are the values of \( h(x) \) at \( x = 1, 2, 3, 4, 5 \):

\[
K_1 = h(1) = (6 + 7 + 10) \mod 13 = 10
\]
\[
K_2 = h(2) = (24 + 14 + 10) \mod 13 = 9
\]
\[
K_3 = h(3) = (54 + 21 + 10) \mod 13 = 7
\]
\[
K_4 = h(4) = (96 + 28 + 10) \mod 13 = 4
\]
\[
K_5 = h(5) = (150 + 35 + 10) \mod 13 = 0
\]
We can recover \( h(x) \) and \( K = h(0) \) from any three of the shadows. For example, using \( K_1, K_3 \) and \( K_5 \) we have:

\[
\begin{align*}
    h(x) &= \left\{ 10 \frac{(x - 3)(x - 5)}{(1 - 3)(1 - 5)} + \\
    &\quad 7 \frac{(x - 1)(x - 5)}{(3 - 1)(3 - 5)} + \\
    &\quad 0 \frac{(x - 1)(x - 3)}{(5 - 1)(5 - 3)} \right\} \mod 13 \\
    &= 10(x - 3)(x - 5)/8 + 7(x - 1)(x - 5)/(-4) \mod 13 \\
    &= 10(x - 3)(x - 5)5 + 7(x - 1)(x - 5)3 \mod 13 \\
    &= 50(x^2 - 8x + 15) + 21(x^2 - 6x + 5) \mod 13 \\
    &= 11(x^2 + 5x + 2) + 8(x^2 + 7x + 5) \mod 13 \\
    &= (19x^2 + 111x + 62) \mod 13 = h(x).
\end{align*}
\]
Asmuth and Bloom Threshold Scheme

Asmuth and Bloom based their threshold scheme on the Chinese Remainder Theorem.

Let $K > 0$ be the key.

Let $p, d_1, d_2, \ldots, d_w$ be integers such that $p > K$, $d_1 < d_2 < \cdots < d_w$, $\gcd(p, d_i) = 1$ for all $i$, $\gcd(d_i, d_j) = 1$ for all $i \neq j$, and $d_1 d_2 \cdots d_t > p d_{w-t+2} d_{w-t+3} \cdots d_w$.

The gcd requirements guarantee that the integers $p, d_1, d_2, \ldots, d_w$ are pairwise relatively prime.

The last condition says that the product of the $t$ smallest $d_i$’s is greater than the product of $p$ and the $t - 1$ largest $d_i$’s. Let $n = d_1 d_2 \cdots d_t$ be the product of the $t$ smallest $d_i$’s. Then $n/p$ is greater than the product of any $t - 1$ of the $d_i$’s.
Let $r$ be a random integer in the range $0 \leq r < n/p$. Write $K' = K + rp$. Then $0 \leq K' < n$. The $w$ shadows are defined as $K_i = K' \mod d_i$ for $i = 1, \ldots, w$.

To recover $K$, it suffices to find $K'$ because $K = K' \mod p$. If $t$ shadows $K_{i_1}, \ldots, K_{i_t}$ are known, then by the Chinese Remainder Theorem, $K'$ is known modulo $n_1 = d_{i_1} \cdots d_{i_t}$. Since $n_1 \geq n \geq K'$, the Chinese Remainder Theorem uniquely determines $K'$.

If only $t-1$ shadows $K_{i_1}, \ldots, K_{i_{t-1}}$ are known, then $K'$ can only be known modulo $n_2 = d_{i_t} \cdots d_{i_{t-1}}$. Because $n/n_2 > p$ (the last condition above) and $\gcd(n_2, p) = 1$, the numbers $x$ such that $x \leq n$ and $x \equiv K' \pmod{n_2}$ are evenly distributed over all the congruence classes modulo $p$. Therefore, there is not enough information to determine $K'$. 
Example of the Asmuth and Bloom Threshold Scheme

Let $K = 3$, $t = 2$, $w = 3$, $p = 5$, $d_1 = 7$, $d_2 = 9$ and $d_3 = 11$. Then $n = d_1 d_2 = 7 \cdot 9 = 63 > 5 \cdot 11 = pd_3$ as required.

We need to choose a random number between 0 and $(63/5)$, that is, between 0 and 12. Picking $r = 9$, we get

$$K' = K + rp = 3 + 9 \cdot 5 = 48.$$  

The shadows are $K_1 = 48 \mod 7 = 6$, $K_2 = 48 \mod 9 = 3$ and $K_3 = 48 \mod 11 = 4$.

Given any two of the three shadows, we can compute $K$. Assume we know $K_1$ and $K_3$. Then $n_1 = d_1 d_3 = 7 \cdot 11 = 77$. The Chinese Remainder Theorem produces $K' \equiv 48 \pmod{77}$. Finally, $K = K' \mod p = 48 \mod 5 = 3$. 