Asmuth-Bloom Threshold Secret Sharing Scheme

Asmuth-Bloom scheme uses special sequences of integers. More exactly, a sequence of pairwise coprime positive integers $p_0, p_1 < \cdots < p_n$ is chosen such that

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

Given a publicly known Asmuth-Bloom sequence, the scheme works as follows:

- The secret S is chosen as a random element of the set $\mathbf{Z}_{p_0}$;
- The shares I_i are chosen as $I_i = (S + \gamma \cdot p_0) \bmod p_i$, for all $1 \leq i \leq n$, where γ is an arbitrary integer such that $S + \gamma \cdot p_0 \in \mathbf{Z}_{p_1 \cdots p_k}$;
- Given k distinct shares $I_{i_1}, \ldots, I_{i_k}$, the secret S can be obtained as $S = x_0 \bmod p_0$, where x_0 is obtained, using the standard variant of the Chinese remainder theorem, as the unique solution modulo $p_{i_1} \cdots p_{i_k}$ of the system

$$\begin{cases} x & \equiv & I_{i_1} \ mod \ p_{i_1} \\ & \vdots & \\ x & \equiv & I_{i_k} \ mod \ p_{i_k} \end{cases}.$$