Feldman's Verifiable Secret Sharing Scheme

Feldman has proposed a non-interactive scheme for achieving verifiability in Shamir's threshold secret sharing scheme. The main idea is to use a one-way function f such that $f(x+y) = f(x) \cdot f(y)$ (it can be proven by induction that $f(ix) = f(x)^i$, for any element x and natural number i) and to broadcast $f(a_0), \ldots, f(a_{k-1})$, where $P(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ is the polynomial used in Shamir's scheme. The consistency of the share $I_i = P(i)$ can be tested by verifying that

$$f(I_i) \stackrel{?}{=} f(a_0) \cdot f(a_1)^{i^1} \cdots f(a_{k-1})^{i^{k-1}}.$$

Indeed, by the homomorphic property of the function f,

$$f(a_0 + a_1 i + \cdots + a_{k-1} i^{k-1}) = f(a_0) \cdot f(a_1)^{i^1} \cdots f(a_{k-1})^{i^{k-1}}.$$

A good candidate for the function f is $f : \mathbf{Z}_q \to \mathbf{Z}_p$, $f(x) = \alpha^x \texttt{ mod } p$, where p and q are odd primes such that $q|(p-1)$, and $\alpha \in \mathbf{Z}_p^*$ is an element of order q. In this case we obtain the following scheme:

- There are generated the primes p and q such that $q|(p-1)$, and $\alpha \in \mathbf{Z}_p^*$ an element of order q. All these numbers are public;
- The dealer generates the polynomial $P(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ over $\mathbf{Z}_q$ such that $a_0 = S$ and makes public $\alpha_i = \alpha^{a_i} \texttt{ mod } p$, for all $0 \le i \le k-1$;
- The dealer securely distributes the share $I_i = P(i)$ to the i^{th} user, for all $1 \le i \le n$;
- Each user can verify the correctness of the received share I_i by testing

$$\alpha^{I_i} \texttt{ mod } p \stackrel{?}{=} \prod_{j=0}^{k-1} \alpha_j^{i^j} \texttt{ mod } p.$$