Bézout's identity:

Let a and b be integers with greatest common divisor d. Then there exist integers x and y such that ax + by = d. Moreover, the integers of the form az + bt are exactly the multiples of d.
Computed by Extended Euclidean algorithm

1. Identify secret message x.
2. Use CRT to distribute shares (r_i, p_i). Note that the shares are non-threshold shares.
3. Publish hash($\Pi\, p_i$) for the verifying purpose.
4. Find a reliable person (P).
5. P publishes his ElGamal model (G, g, K_p).
    a. G is a multiplicative group (mod x).
    b. g is a generator.
    c. K_p is $g^p mod\ x$ - can't calculate p from K_p.
6. For each shareholder:
    a. Find a random number as their own key, K_{ei}
    b. Publish $p_i * K_p^{K_{ei}}$ and $g^{K_{ei}} mod\, x$
7. P gathers data, compute $\Pi\, p_i * K_p^{K_{ei}}$ and $\Pi\, g^{K_e}$
8. DA how has $p_1 * p_2 *... * p_n * K_p^{K_{e1}+K_{e2}+...+K_{en}}$ and $g^{K_{e1}+K_{e2}+...+K_{en}}$
9. Simplify: $p_1 * p_2 *... * p_n * g^{p(K_{e1}+K_{e2}+...+K_{en})}$
10. Calculate $(g^{K_{e1}+K_{e2}+...+K_{en}})^p = g^{p(K_{e1}+K_{e2}+...+K_{en})}$
11. DA finds $(g^{p(K_{e1}+K_{e2}+...+K_{en})})^{-1}$ and multiplies that with $p_1 * p_2 *... * p_n * K_p^{K_{e1}+K_{e2}+...+K_{en}}$ to get the product of the prime numbers. Verify it with the hash code.

Trusted P: Publish g^p.

Shareholder: Calculate $g^{K_{ei}}$ and $p * (g^p)^{K_{ei}} = p_1 * g^{p*K_{ei}}$

Trusted P: multiply from each shareholder and get $g^{K_{e1}+K_{e2}+...+K_{en}}$ and $p_1 * p_2 *... * p_n * g^{p(K_{e1}+K_{e2}+K_{e3}+...+K_{en})}$

Now we only need to find the inverse of $g^{p(K_{e1}+K_{e2}+K_{e3}+...+K_{en})}$.

We can find $g^{p(K_{e1}+K_{e2}+K_{e3}+...+K_{en})}$ by calculating $g^{K_{e1}+K_{e2}+...+K_{en}}{}^p$.
And then find the inverse and get $p_1 * p_2 *... * p_n$.

Put the product into hash function and compare the hash result.