ANALYSIS AND OBSERVATION

Shamir's secret sharing scheme is designed to share a single secret value sj among n servers such that shares must be obtained from any k servers in order to reconstruct sj. The scheme's security rests on the fact that at least k points are needed to uniquely reconstruct a polynomial of degree k – 1.

Yes, it will withstand the frequency analysis attack. Another implicit assumption made is that the sample size (length of encrypted message) has to be large enough for a frequency analysis to be accurate. If the encrypted message is short then it would be difficult for an analysis attack to have any significant implications (unless of course, the possible number of inputs are small as well). It should be noted that most modern encryption are well-defended against frequency analysis attacks.

Changes that can be made to make SSS more secure against frequency analysis attack we can chose a parameter set based on the minimum number of shares to supposedly provide protection against any univariate attack. If X and p are public, and k or more servers collude then it will be easy to attack and hence we can make it secure by keeping X and p as private.

Bonus

No, it possible to perform the above homomorphic operations using RSS.

Ramp secret sharing (SS) schemes can be classified into strong ramp SS schemes and weak ramp SS schemes. The strong ramp SS schemes do not leak out any part of a secret explicitly even in the case where some information about the secret leaks from a non-qualified set of shares, and hence, they are more desirable than weak ramp SS schemes. However, it is not known how to construct the strong ramp SS schemes in the case of general access structures. It is pointed out that threshold ramp SS schemes based on Shamir's polynomial interpolation method are not always strong.