

G , a subgroup of the multiplicative group of a finite field F_p^*