Ciphertext overflow detection zones

No overflow detection zones

Attacked $c$

$p + (\zeta + 1)^d (M + \kappa^2)^d$

Unattacked $c \bmod p$

Ciphertext overflow

$p$

upper bound $(\zeta + 1)^d (M + \kappa^2)^d$

$\bmod p$

Frequency

Frequency