

Table 1: Conventions for All Protocols

A, B, S	Principal members Alice, Bob, Sally
PK_p, SK_p	is a public, private key pair of principal p
$\text{auth-}PK_p, \text{auth-}SK_p$	key pair of any principal P for Authentication
$\text{eval-}PK, \text{eval-}SK$	key pair generated by FHE scheme
$func(x)$	is an arbitrary function
data, x, y	users data, input, output respectively to $func$
data^1, x^1, y^1	are encryptions of data, x, y respectively
$\text{encrypt}, \text{decrypt}, \text{evaluate}$	methods of FHE scheme
$\text{sign}, \text{verify}$	signature and verify operations