| Protocols | Party | Offline Comp. | Online Comp. | Comm.trans (in bit |
|---|---|---|---|---|
|  | Initiator | $(2m+2m^2)exp_1$, $(2m)h$ | $(m+m^2)exp_1$, $(m)h$ | $3m \cdot 1024$ |
|  | Responder | $(m+m^2)exp_1$, $(2m)h$ | $(2m)exp_1$ | $4m \cdot 1024$ |
|  | Initiator | $(2rm)exp_1$, $(rm)exp_2$ | $(rm)exp_1$, $(2rm)exp_2$ | $rm \cdot 2048$ |
|  | Responder | —- | $(2rm+1)exp_1$, $(2rm+1)exp_2$ | $rm \cdot 2048$ |
| P-match | Initiator | $(2m+1)exp_1$, $(m)h$ | $(2m)exp_1$ | $4m \cdot 1024$ |
|  | Responder | $(2m+1)exp_1$, $(m)h$ | $(3m)exp_1$ | $2m \cdot 1024$ |
| E-match | Initiator | $(2m)h$, $1poly^+$ | —- | 1024 |
|  | Responder | $(rm)h$, $((r-1)m)mul_1$ | $(rm)poly^-$ | 32 |