

Figure 1

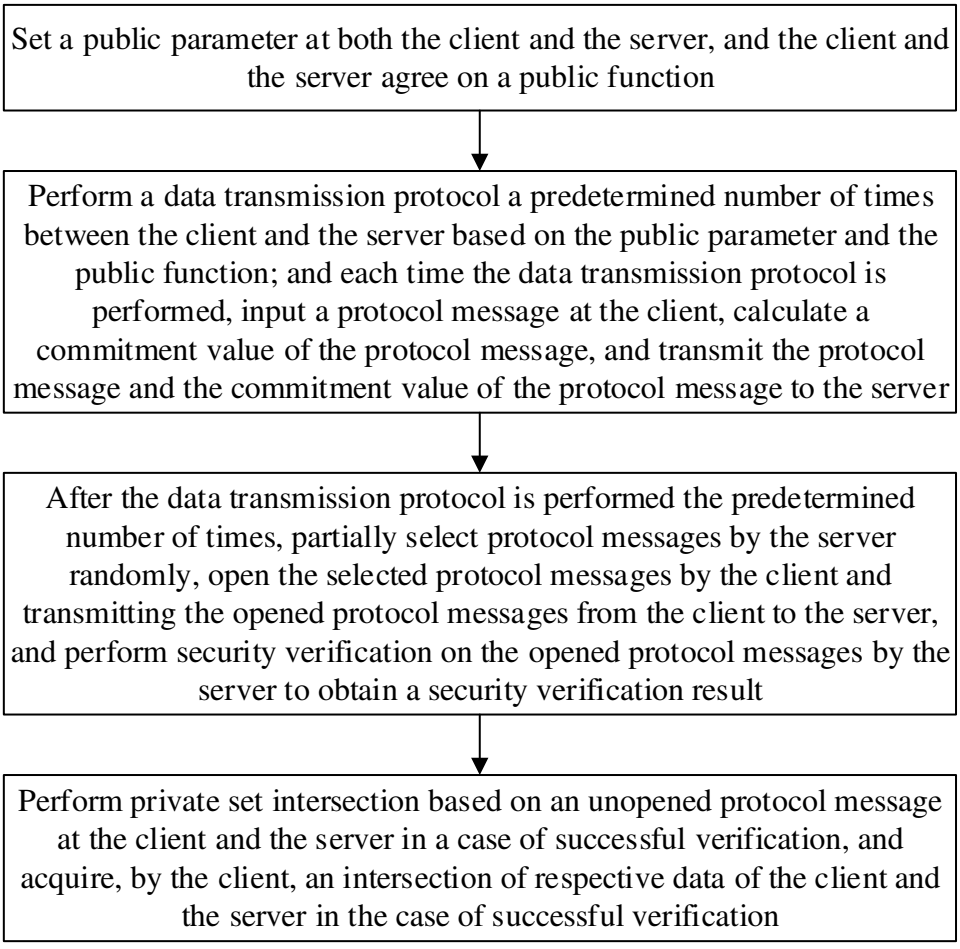


Figure 2

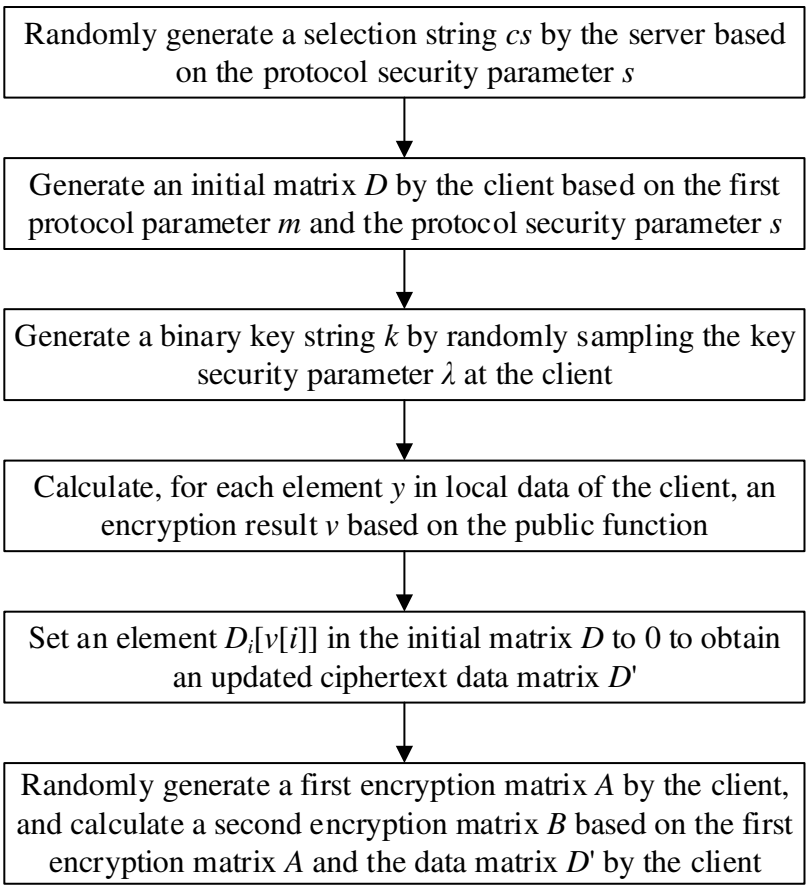

Randomly generate a selection string cs by the server based on the protocol security parameter s
Generate an initial matrix D by the client based on the first protocol parameter m and the protocol security parameter s
Generate a binary key string k by randomly sampling the key security parameter λ at the client
Calculate, for each element y in local data of the client, an encryption result v based on the public function
Set an element $D_i[v[i]]$ in the initial matrix D to 0 to obtain an updated ciphertext data matrix D'
Randomly generate a first encryption matrix A by the client, and calculate a second encryption matrix B based on the first encryption matrix A and the data matrix D' by the client

Figure 3

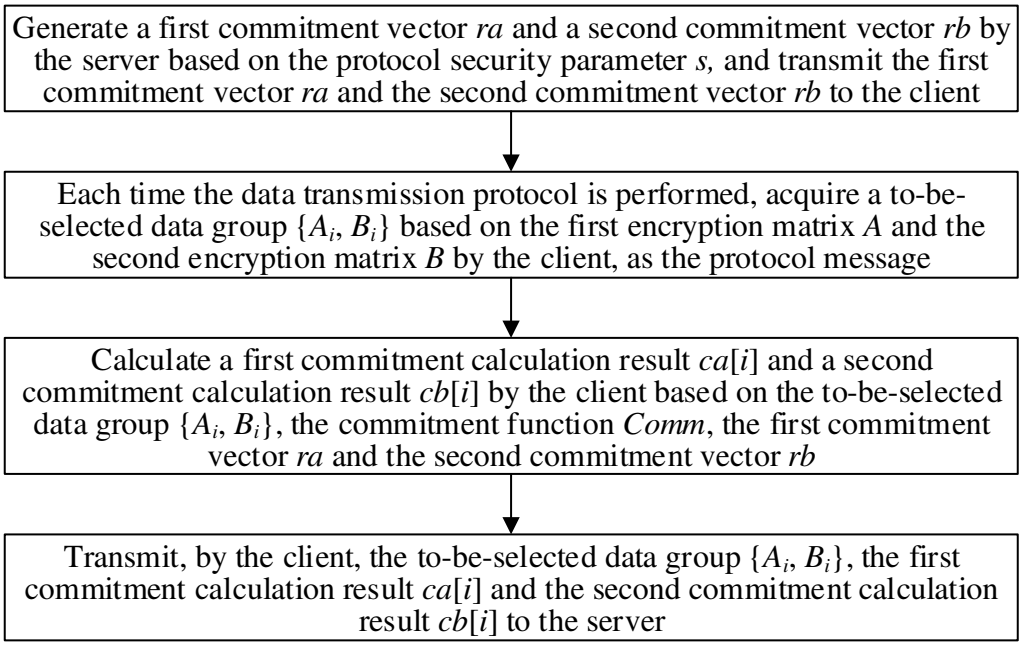

Generate a first commitment vector ra and a second commitment vector rb by the server based on the protocol security parameter s, and transmit the first commitment vector ra and the second commitment vector rb to the client
Each time the data transmission protocol is performed, acquire a to-be-selected data group {Ai, Bi} based on the first encryption matrix A and the second encryption matrix B by the client, as the protocol message
Calculate a first commitment calculation result ca[i] and a second commitment calculation result cb[i] by the client based on the to-be-selected data group {Ai, Bi}, the commitment function Comm, the first commitment vector ra and the second commitment vector rb
Transmit, by the client, the to-be-selected data group {Ai, Bi}, the first commitment calculation result ca[i] and the second commitment calculation result cb[i] to the server

Figure 4

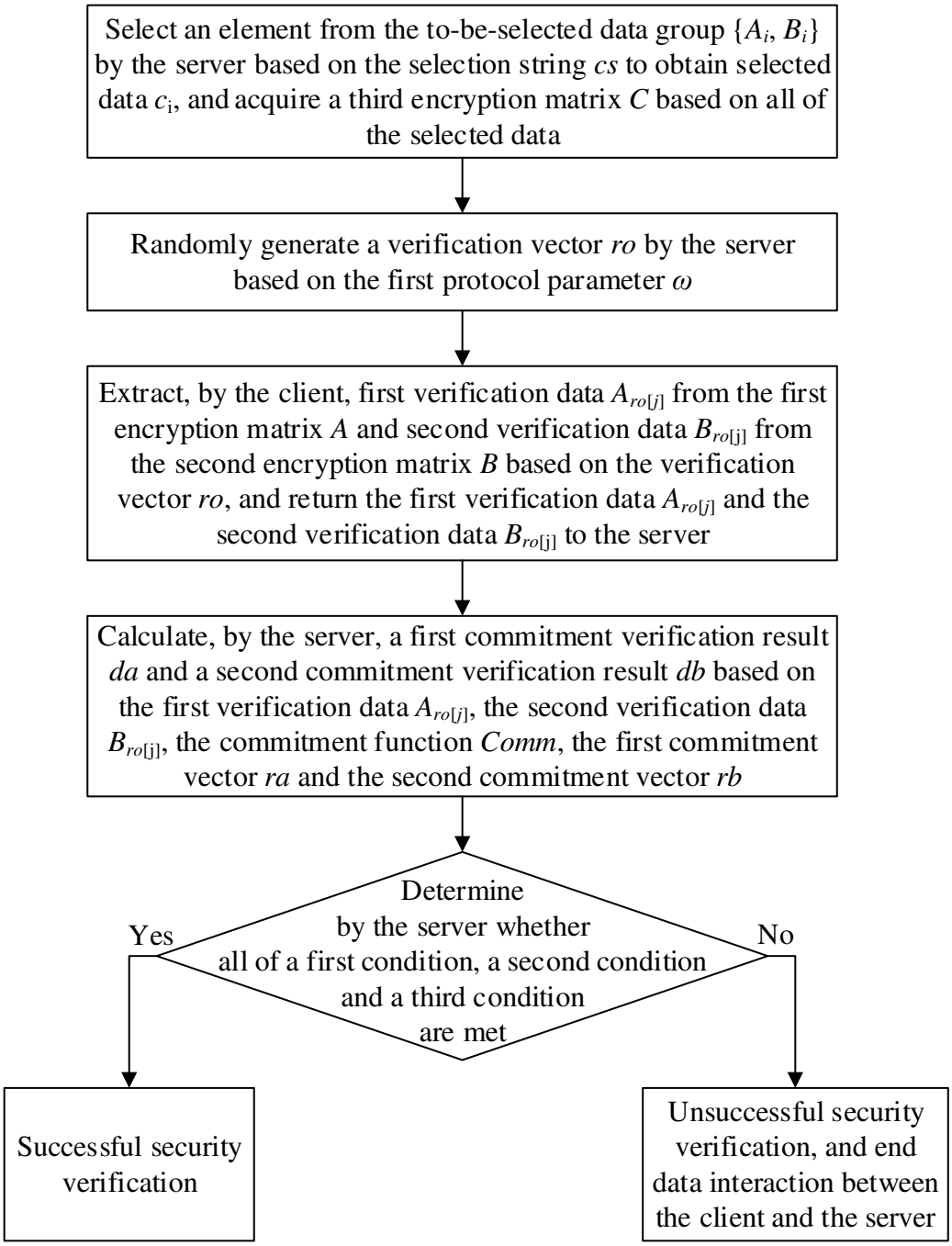

Select an element from the to-be-selected data group {A_i, B_i} by the server based on the selection string *cs* to obtain selected data c_i, and acquire a third encryption matrix *C* based on all of the selected data
Randomly generate a verification vector *ro* by the server based on the first protocol parameter ω
Extract, by the client, first verification data $A_{ro[j]}$ from the first encryption matrix *A* and second verification data $B_{ro[j]}$ from the second encryption matrix *B* based on the verification vector *ro*, and return the first verification data $A_{ro[j]}$ and the second verification data $B_{ro[j]}$ to the server
Calculate, by the server, a first commitment verification result *da* and a second commitment verification result *db* based on the first verification data $A_{ro[j]}$, the second verification data $B_{ro[j]}$, the commitment function *Comm*, the first commitment vector *ra* and the second commitment vector *rb*
Determine by the server whether all of a first condition, a second condition and a third condition are met
Yes
No
Successful security verification
Unsuccessful security verification, and end data interaction between the client and the server

Figure 5

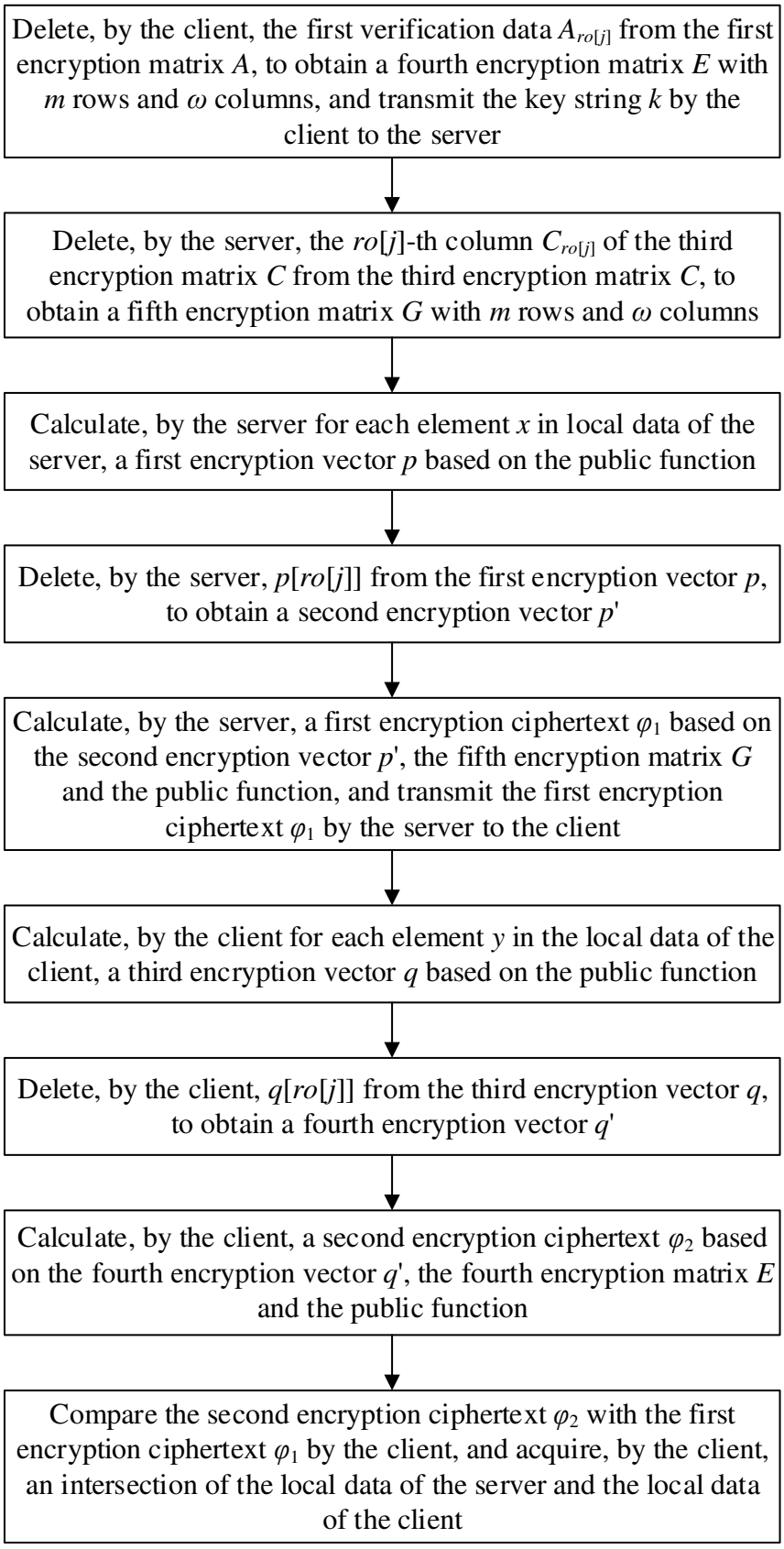

Delete, by the client, the first verification data $A_{ro[j]}$ from the first encryption matrix A, to obtain a fourth encryption matrix E with m rows and ω columns, and transmit the key string k by the client to the server
Delete, by the server, the $ro[j]$-th column $C_{ro[j]}$ of the third encryption matrix C from the third encryption matrix C, to obtain a fifth encryption matrix G with m rows and ω columns
Calculate, by the server for each element x in local data of the server, a first encryption vector p based on the public function
Delete, by the server, $p[ro[j]]$ from the first encryption vector p, to obtain a second encryption vector p'
Calculate, by the server, a first encryption ciphertext φ_1 based on the second encryption vector p', the fifth encryption matrix G and the public function, and transmit the first encryption ciphertext φ_1 by the server to the client
Calculate, by the client for each element y in the local data of the client, a third encryption vector q based on the public function
Delete, by the client, $q[ro[j]]$ from the third encryption vector q, to obtain a fourth encryption vector q'
Calculate, by the client, a second encryption ciphertext φ_2 based on the fourth encryption vector q', the fourth encryption matrix E and the public function
Compare the second encryption ciphertext φ_2 with the first encryption ciphertext φ_1 by the client, and acquire, by the client, an intersection of the local data of the server and the local data of the client

Figure 6