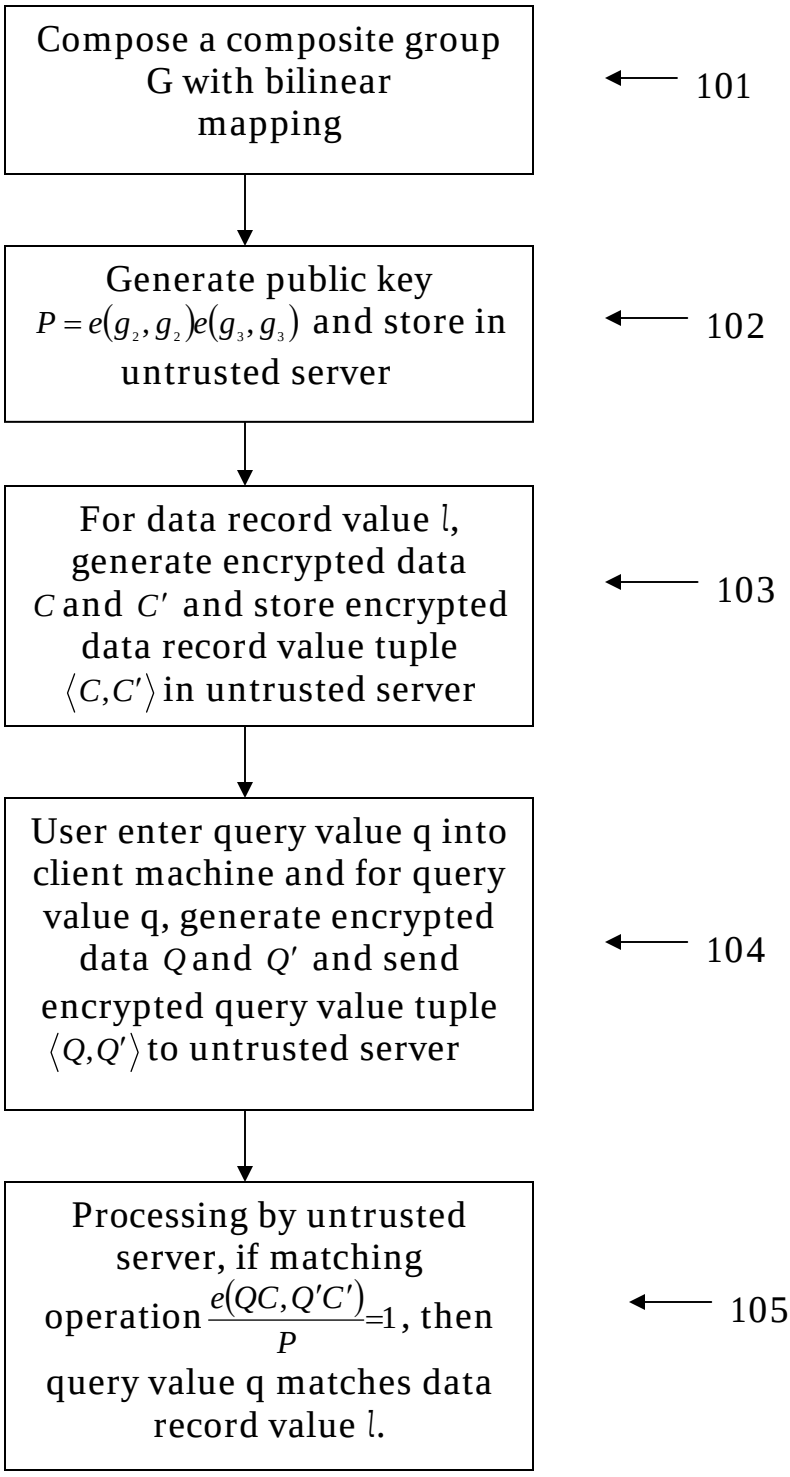
Compose a composite group G with bilinear mapping
101
Generate public key $P = e(g_2, g_2)e(g_3, g_3)$ and store in untrusted server
102
For data record value l, generate encrypted data C and C' and store encrypted data record value tuple $\langle C, C' \rangle$ in untrusted server
103
User enter query value q into client machine and for query value q, generate encrypted data Q and Q' and send encrypted query value tuple $\langle Q, Q' \rangle$ to untrusted server
104
Processing by untrusted server, if matching operation $\frac{e(QC, Q'C')}{P}=1$, then query value q matches data record value l.
105

Fig. 1

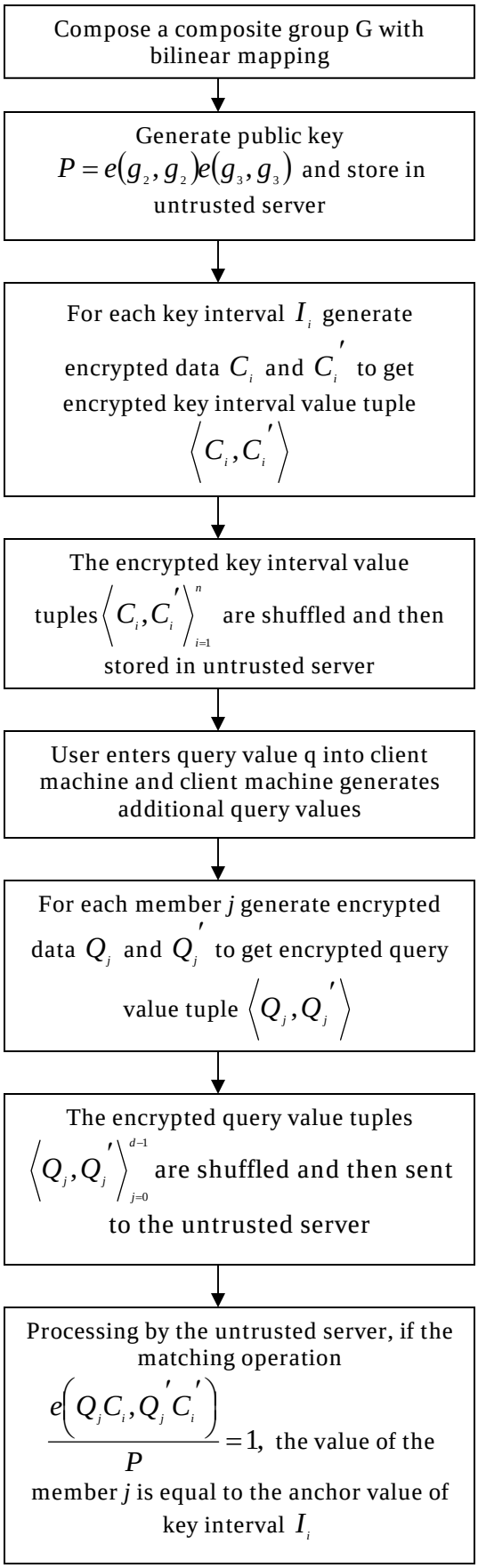
Compose a composite group G with bilinear mapping
201
Generate public key $P = e(g_2, g_2)e(g_3, g_3)$ and store in untrusted server
202
For each key interval I_i generate encrypted data C_i and C_i' to get encrypted key interval value tuple $\langle C_i, C_i' \rangle$
203
The encrypted key interval value tuples $\langle C_i, C_i' \rangle_{i=1}^{n}$ are shuffled and then stored in untrusted server
204
User enters query value q into client machine and client machine generates additional query values
205
For each member *j* generate encrypted data Q_j and Q_j' to get encrypted query value tuple $\langle Q_j, Q_j' \rangle$
206
The encrypted query value tuples $\langle Q_j, Q_j' \rangle_{j=0}^{d-1}$ are shuffled and then sent to the untrusted server
207
Processing by the untrusted server, if the matching operation $\frac{e(Q_j C_i, Q_j' C_i')}{P} = 1$, the value of the member *j* is equal to the anchor value of key interval I_i
208

Fig. 2