B8： (选项)计算 $S_2=Hash(0x83\|g_1\|Hash(g_2\|g_3\|ID_A\|ID_B\|R_A\|R_B))$，并检验 $S_2=S_A$ 是否成立，若等式不成立则从 A 到 B 的密钥确认失败。

## 4.2 密钥交换协议流程

密钥交换协议流程如图1。

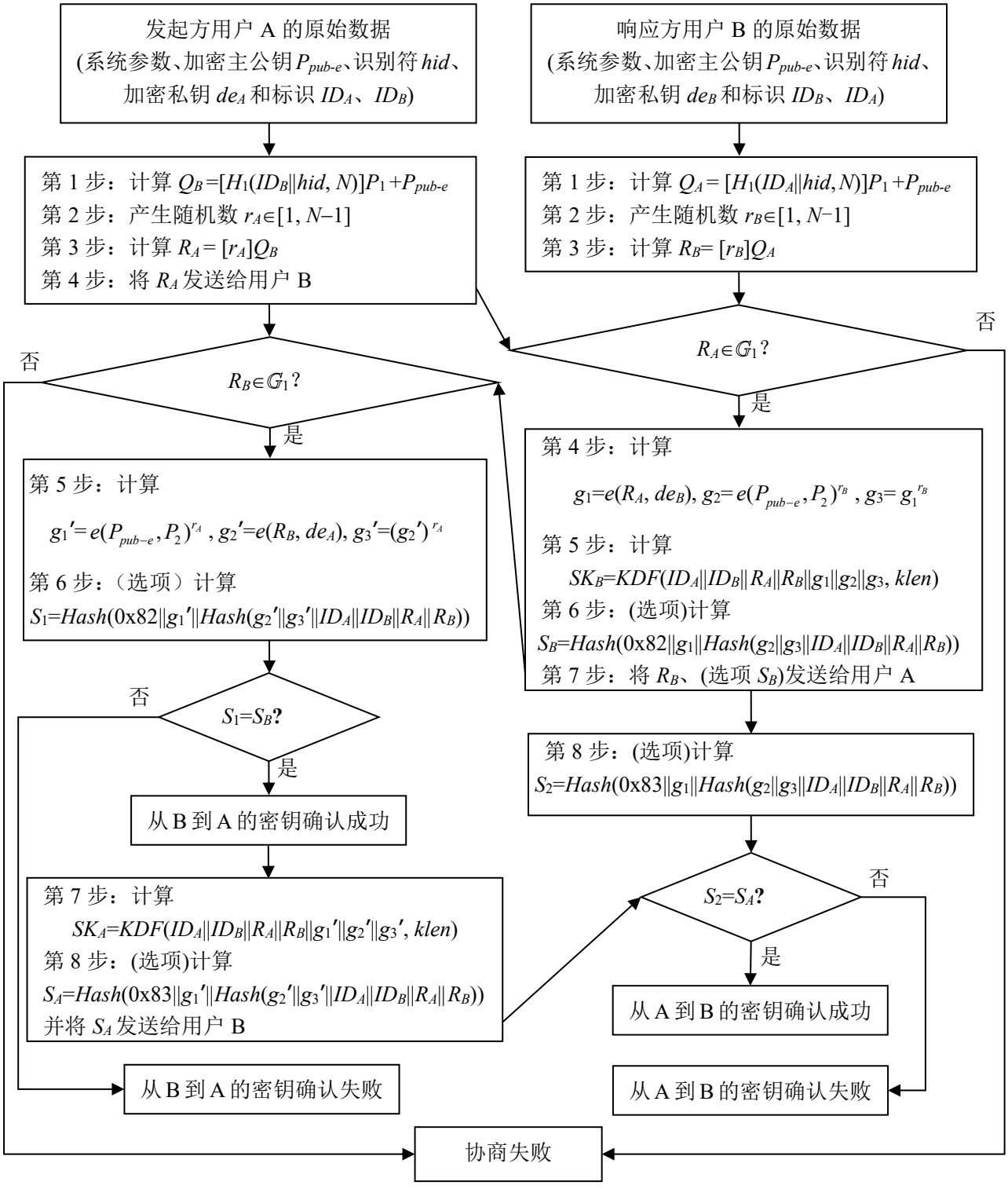


图 1 密钥交换协议流程