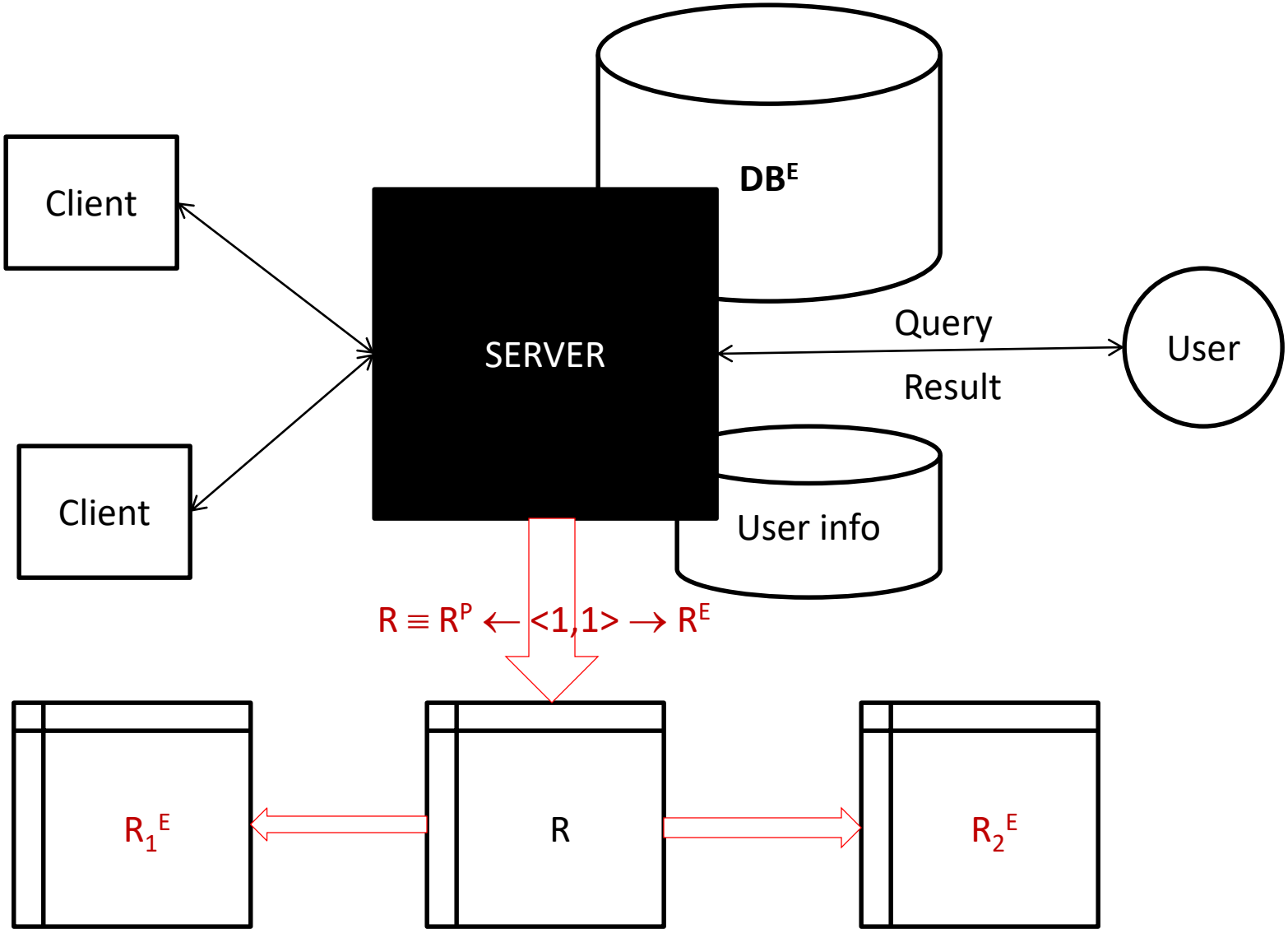
DBS-classical approaches

Lecture 6

Client-Server Model



User Information Protection

- User passwords are stored as hashes.
- Data in transit for the authentication phase must be protected (using SSL/Public key cryptosystems).

Chinese Remainder Theorem

- Database D = <F1,…, Fn>
- Phase 1: Encrypt database
  1. Chose n primes p1,…, pn: pi > Fi, i=1,…, n. Send pi to Useri.
  2. Solve the congruent system $C \equiv Fi \pmod{pi}$, i=1,…,n, for C.
  3. Return C
- Phase 2: Read
  1. Fi = C mod pi, $\forall 1 \leq i \leq n$.

Threshold Model

- θ(m, n) model: There are n members who share a secret X. Each member keeps only part of the secret and no member knows X. X can only be decrypted when at least m, m $\leq$ n, members share their secrets.
- θ(m, n) model can implement using the Chinese Remainder Theorem or interpolation Lagrange.