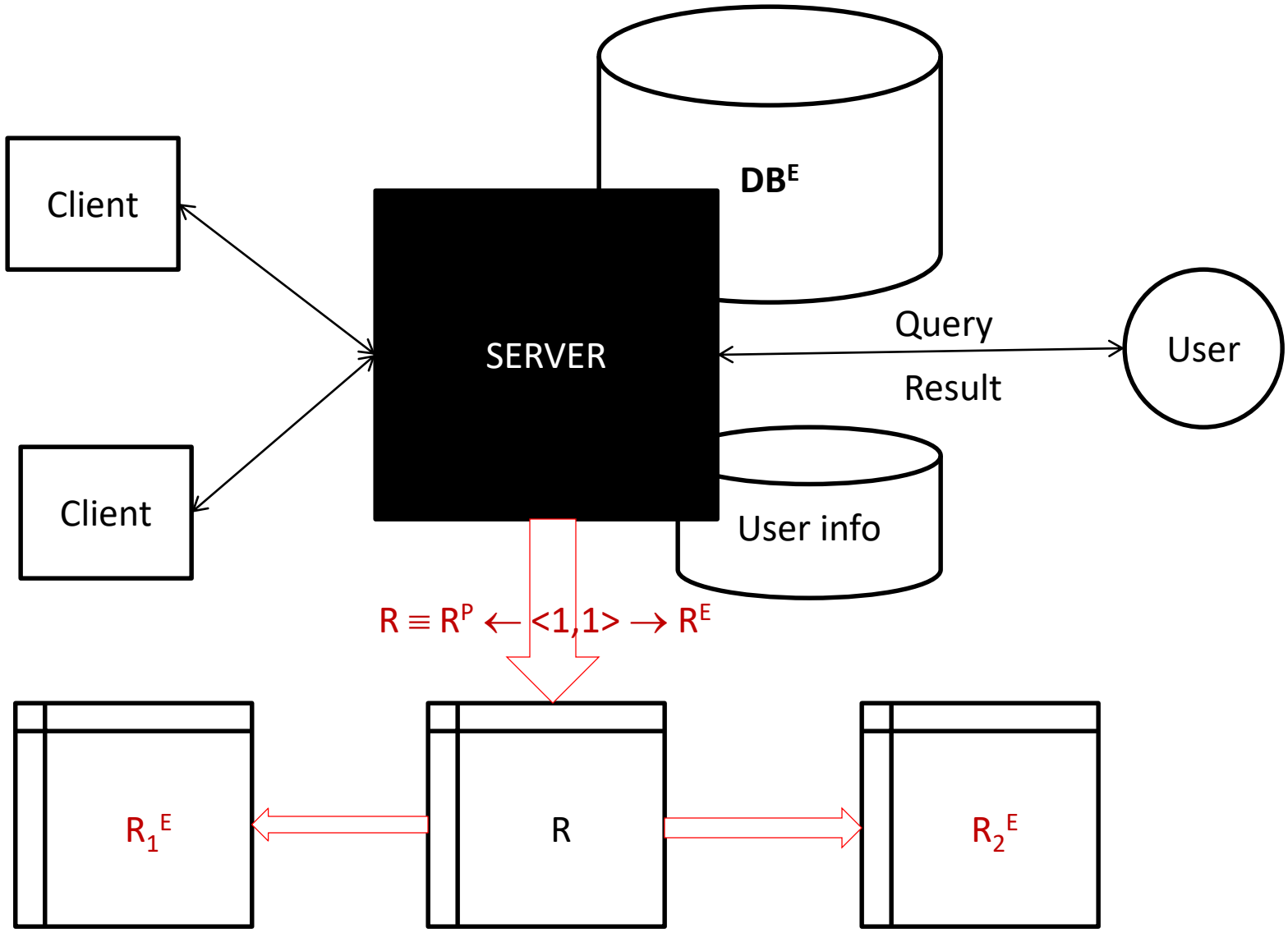
Secure index for numeric data

Lecture 8

Risk model

Assume that client, user are trusted.



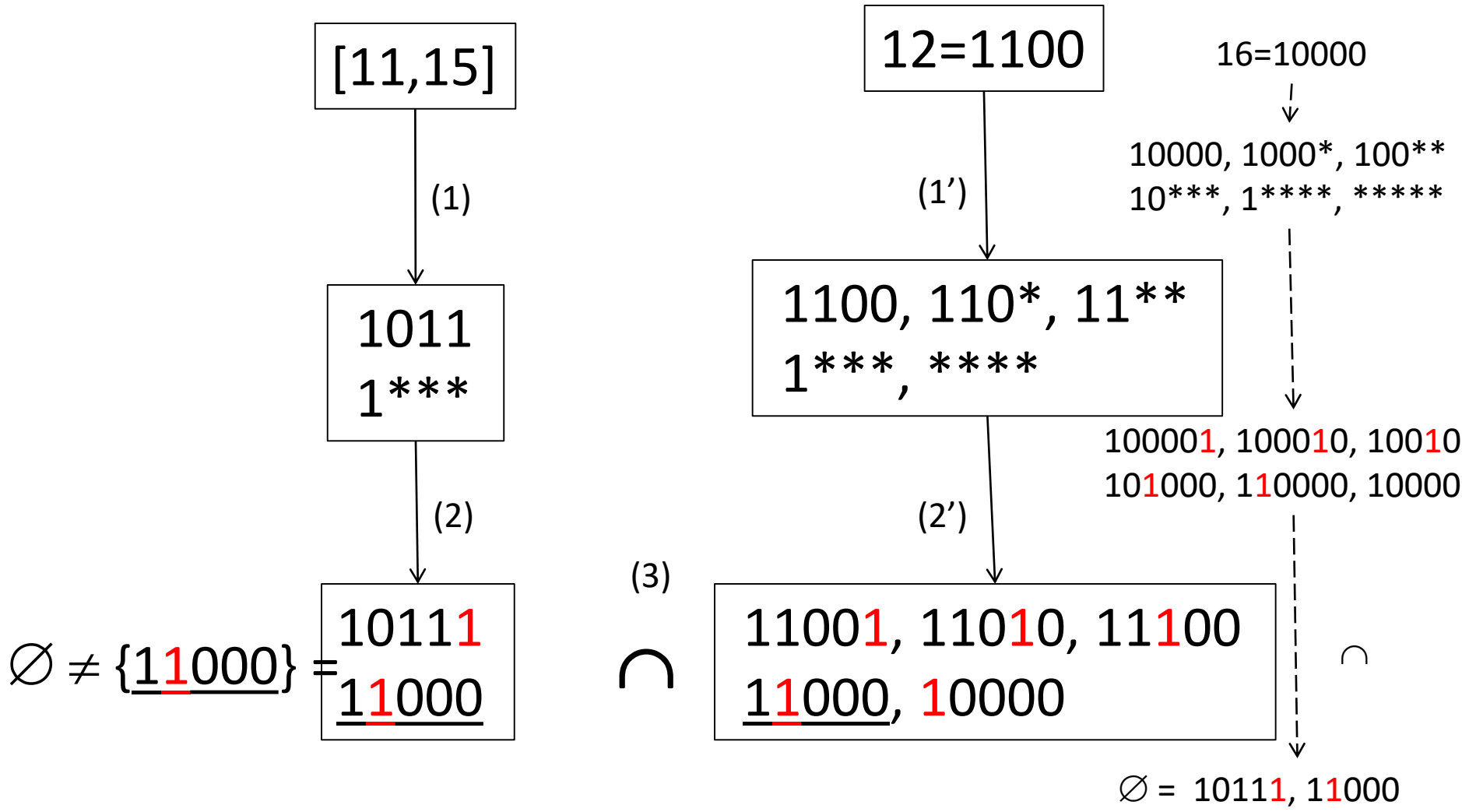
Representing an integer

- k-prefix string: k high bits are fixed, and w-k low are free by pattern $\{0/1\}^k\{*\}^{w-k}$.
- k-bit string represents a set of 2^{w-k} strings with the same high k bits. For example 1**={100, 101, 110, 111}.
- Given $x \in N$, a family of prefix for x is defined by $F(x)=F(b_1 \ldots b_w)=\{b_1 \ldots b_{w-i+1}***\}_i$. For example F(12)=F(1100)={1100, 110*, 11**, 1***, ****}.
- Given an integer x and a prefix P, $x \in P \Leftrightarrow P \in F(x)$.

Representing a range

- S([a,b]) is the smallest set of prefix P_i such that $\cup_l P_i = [a, b]$. For example S([11,15])={1011,11**}.
- Given x and [a,b], $x \in [a,b] \Leftrightarrow F(x) \cap S([a,b]) \neq \emptyset$.
- Given prefix P. N(P) is bit string such that for all pair of prefix P1 and P2, P1=P2⇔N(P1)=N(P2).
- There are many definitions for N. This is a definition: $N(b_1 \ldots b_k * \ldots *) = b_1 \ldots b_k 1_{k+1} 0 \ldots 0_{w+1}$.
- Given x and [a,b], $x \in [a,b] \Leftrightarrow N(F(x) \cap N(S[a,b]) \neq \emptyset$.

Example: check if $12 \in [11,15]$



Protocols

Submit data (t, list)

1. Sort(list): $d_0<d_1<\ldots<d_{n+1}$.
2. Compute $\{S[d_i,d_{i+1}]\}_{i=0,\ldots,n}$.
3. Compute $\{N(S[d_i,d_{i+1}])\}_i$.
4. Compute $\{H(N(S[d_i,d_{i+1}]))\}_i$.
5. Encrypt $\{c_i=E(d_i)\}_i$.
6. Send to server $\{(c_i,H(N(S[d_i,d_{i+1}])))\}_i$.

Query Q(t,[a,b]), $d_0<a\leq b<d_{n+1}$.

1. Compute F(a), F(b).
2. Compute N(F(a)), N(F(b)).
3. Compute H(N(F(a)), N(F(b)).
4. Send {t,H(N(F(a)),H(N(F(b))}

Query processing

(exercise)