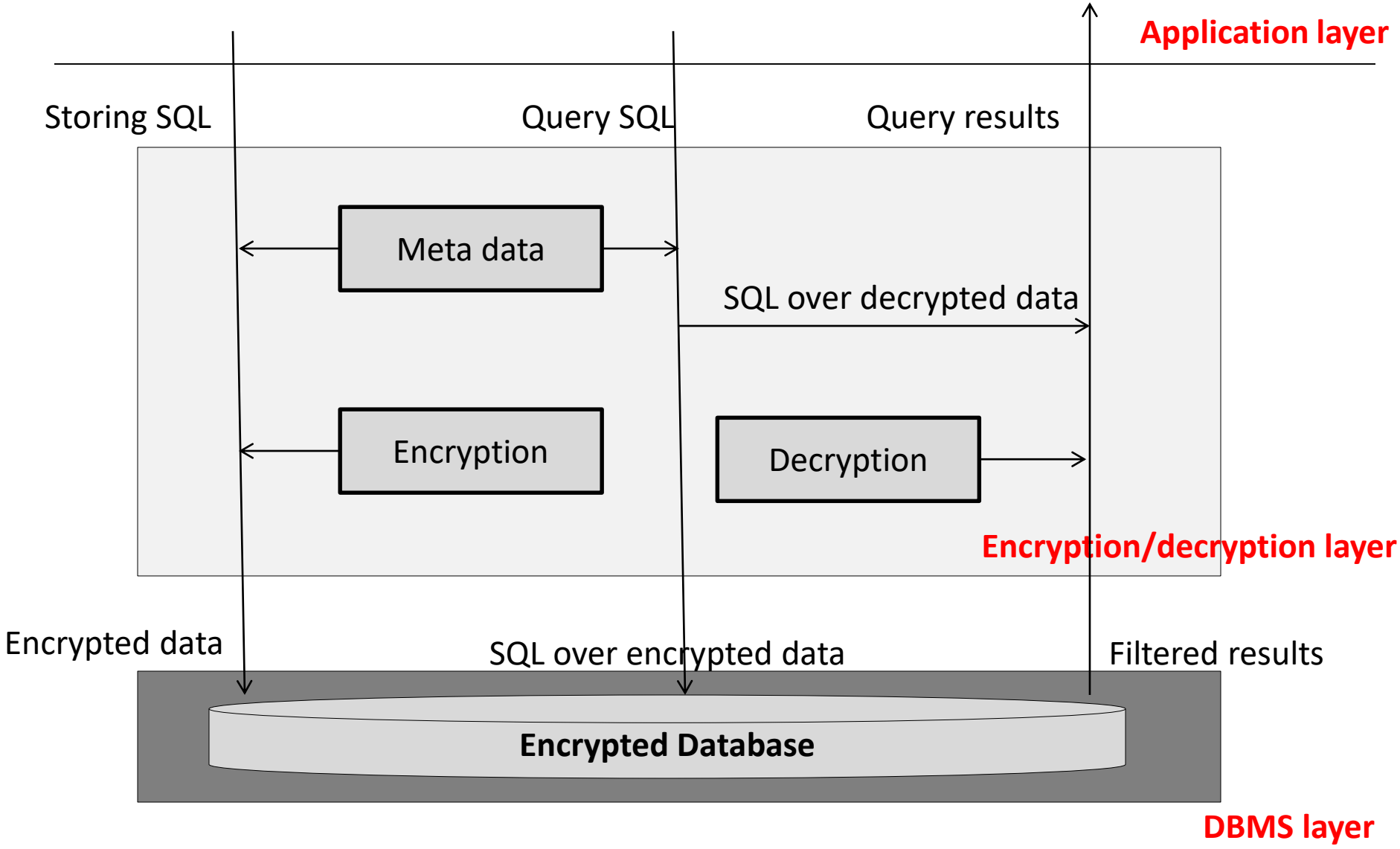
DBS – Secure Index

Lecture 7

System architecture



2-phase scheme

- First phase
  1. Translate/encrypt query using meta data
  2. Execute encrypted query over encrypted database
  3. Return filtered DB (via secure index)
- Second phase
  1. Decrypt the filtered DB
  2. Execute query over decrypted DB
  3. Return results

Secure index for characteristic data

- Pair Coding Function:

$$PC: Alphabet^{*} \rightarrow \{0, 1\}^{m}$$

$$PC(S=c_1c_2\ldots c_n) = (Index=b_0b_1\ldots b_m)$$

where $b_j = 1$ if $H(c_jc_{j+1})=i$ else $b_j = 0$.

- Encrypted storage

  . $R(X_1,\ldots,X_s,\ldots,X_N)$: plain database, where X_s is the sensitive attribution

  . $R^E(X_1,\ldots,X_s^E,\ldots X_N,X_s^I)$, where $X_s^E=Enc(X_s)$, $X_s^I=PC(X_s)$

Query over encrypted data

- Translate plain query to secure index and execute over encrypted database via secure index.
- Translation functions
  - Trans(A_s.v) $\Rightarrow$ A_s^I = PC(v)
  - Trans(A_s like $c_1 \ldots c_k$) $\Rightarrow$ $\wedge_{i=1,\ldots,k}((A_s^I)_{H(cic(i+1))}=1$
  - Trans(A_s not like $c_1 \ldots c_k$) (exercise)
- Compound queries with boolean operation (exercise)

Secure index for numeric data

- Labeled data:

$$L: [a, b] \rightarrow \{1,\ldots,k\}$$

$$L(a_i \leq x < a_{i+1}) = i \text{ where}$$

$[a_1=a,a_2),[a_2,a_3),\ldots,[a_{k-1},a_k=b]$ is a partition of $[a, b]$

- Encrypted storage

  . $R(X_1,\ldots,X_s,\ldots,X_N)$: plain database, where X_s is the sensitive attribution

  . $R^E(X_1,\ldots,X_s^E,\ldots X_N,X_s^I)$, where $X_s^E=Enc(X_s)$, $X_s^I=L(X_s)$

- Query over encrypted data (exercise)