

数据库系统概论新技术篇

数据库安全

秦 波

中国人民大学信息学院

2017年4月



数据库安全

目录

Contents

1 数据库安全基础

2 细粒度访问控制

3 加密数据查询或访问

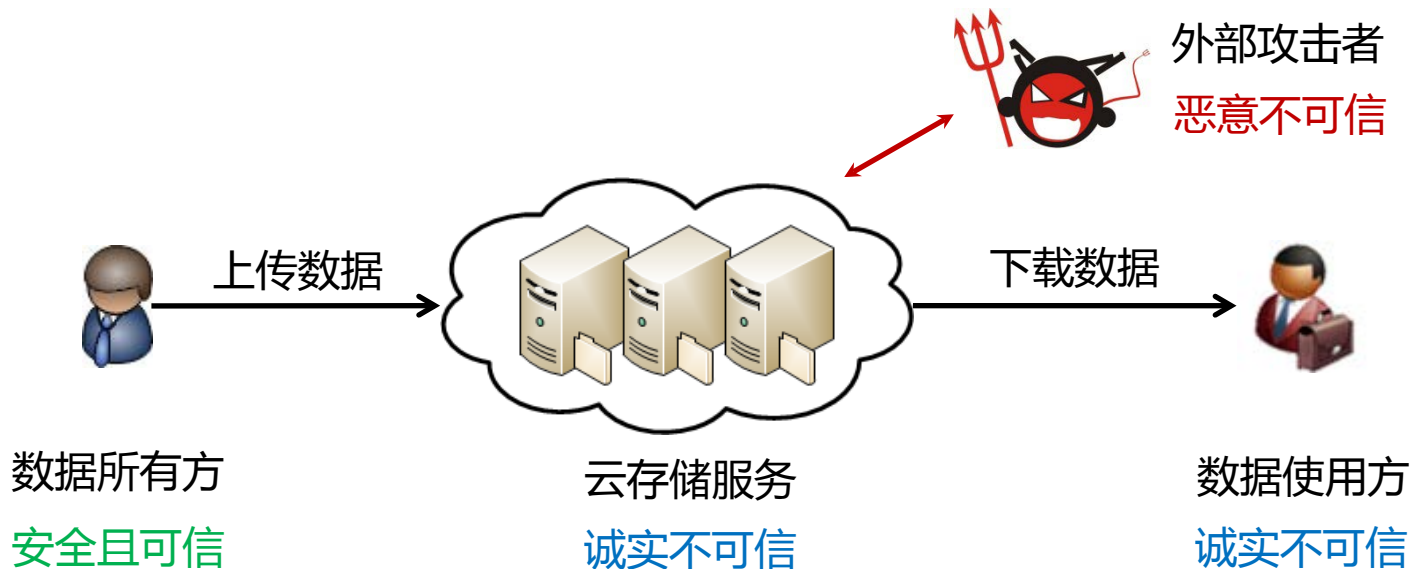
4 隐私保护数据发布

5 隐私保护统计数据发布

6 总结与展望

2 加密细粒度访问控制体系架构

- **安全且可信**：可正确执行算法或步骤，不会泄露自己的秘密信息，可信
- **诚实不可信**：可正确执行算法或步骤，会对系统实施恶意攻击，不可信
- **恶意不可信**：可对系统进行任意的攻击行为，可和诚实不可信实体合谋





数据库安全

目录

Contents

2.1 属性加密

2.2 谓词加密

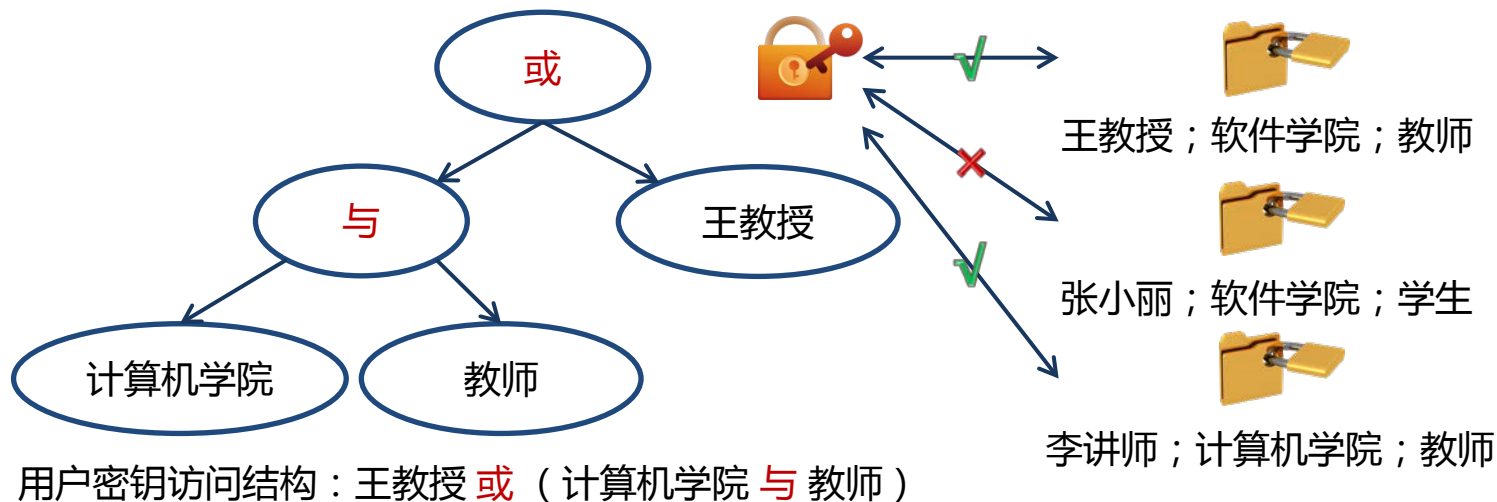
2.3 函数加密

2.4 实例

2.1 属性加密 (Attribute-Based Encryption , ABE)

- **功能**：允许为加密数据指定访问控制树描述的访问结构
- **方法**：使用属性集合或访问结构对信息进行加密
仅当属性集合满足访问结构时，数据才可被解密
- **分类**：密钥策略属性加密 (KP-ABE)，密文策略属性加密 (CP-ABE)

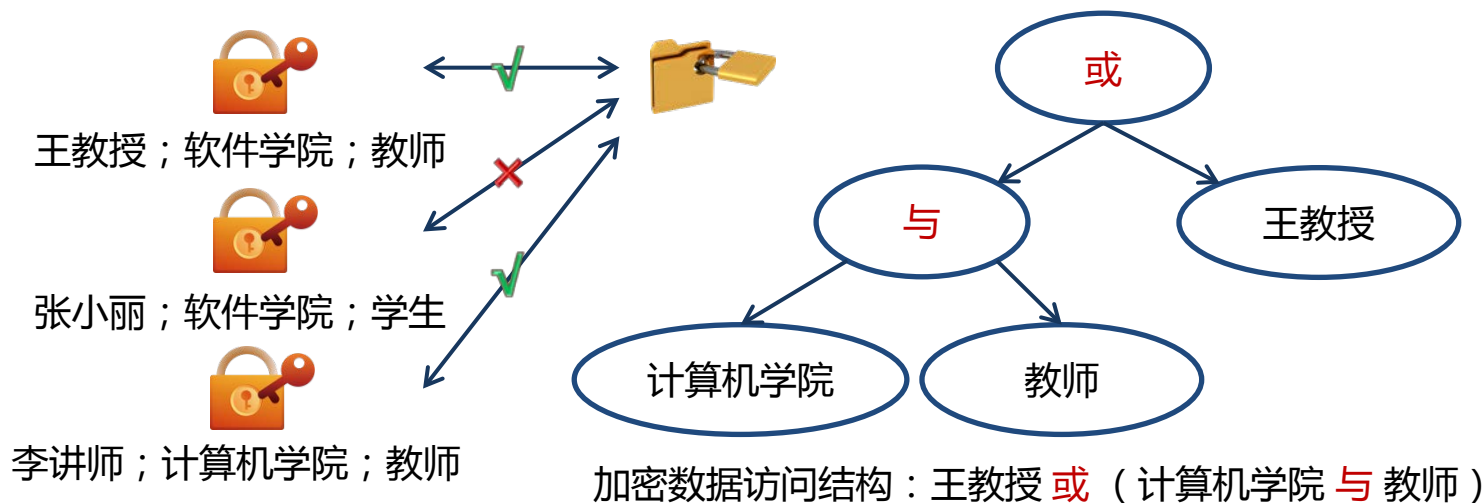
KP-ABE：访问结构与用户密钥绑定，属性集合与加密数据绑定



2.1 属性加密 (Attribute-Based Encryption , ABE)

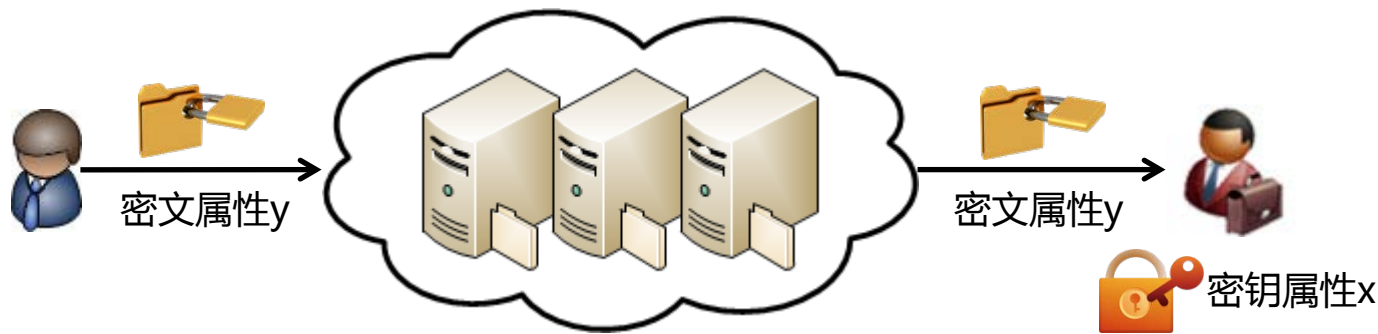
- **功能**：允许为加密数据指定访问控制树描述的访问结构
- **方法**：使用属性集合或访问结构对信息进行加密
仅当属性集合满足访问结构时，数据才可被解密
- **分类**：密钥策略属性加密 (KP-ABE)，密文策略属性加密 (CP-ABE)

CP-ABE：访问结构与加密数据绑定，属性集合与用户密钥绑定



2.2 谓词加密 (Predicate Encryption , PE)

- **功能**：允许为加密数据指定用任意谓词关系 $P(x, y) = \{0, 1\}$ 描述的访问结构
- **方法**：使用密文属性 x 对信息进行加密，用户私钥与密钥属性 y 关联
仅当密钥属性 x 与密文属性 y 满足 $P(x, y) = 1$ 时，数据才可被解密
- **分类**：ABE功能的进一步扩展，是加密数据细粒度访问控制的一般化形式



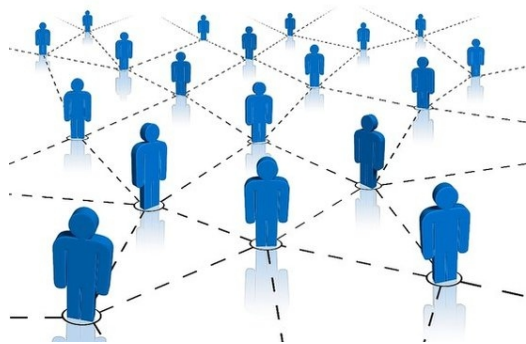
当 $P(x, y) = 1$ 时，解密成功，数据使用方得到解密数据
当 $P(x, y) = 0$ 时，解密失败，数据使用方无法获取信息

2.3 函数加密 (Functional Encryption, FE)

- **功能**：允许在用户密钥中指定某一函数 f ，解密数据 x 的加密结果可得到 $f(x)$
- **特点**：解密结果并非为原始数据 x ，而是数据 x 经过函数 f 后的处理结果。
此功能一旦实现，将为云计算提供绝佳的安全计算方法
- **进展**：函数加密仍处于研究阶段，现有构造方案实现较为复杂
- **难点**：解密过程中，数据使用方不能得到 x 的任何信息，只能得到 $f(x)$

实例1：上传数据 x 为用户加密社交信息，函数 $f(x)$ 返回用户可能认识的朋友

实例2：上传数据 x 为用户个人加密照片，函数 $f(x)$ 返回照片模糊化结果



2.4 实例：Advanced Crypto Software Collection

- **简介**：面向安全系统工程师的高级密码学工具库，由著名密码学家们维护
- **链接**：<http://hms.isi.jhu.edu/acsc/>

| 已包含工具库 | 对应方案 | 实现语言 |
|--|-----------------|--------|
| Ciphertext-Policy Attribute-Based Encryption | 密文策略属性加密 | C |
| Broadcast Encryption | 广播加密，谓词加密特例 | C |
| PIRATTE | 具有密钥撤销功能的属性加密方案 | C |
| Charm | 多个谓词加密特例实现 | Python |
| PBC Library | 各谓词加密底层数学库 | C |



数据库安全

目录

Contents

1 数据库安全基础

2 细粒度访问控制

3 加密数据查询

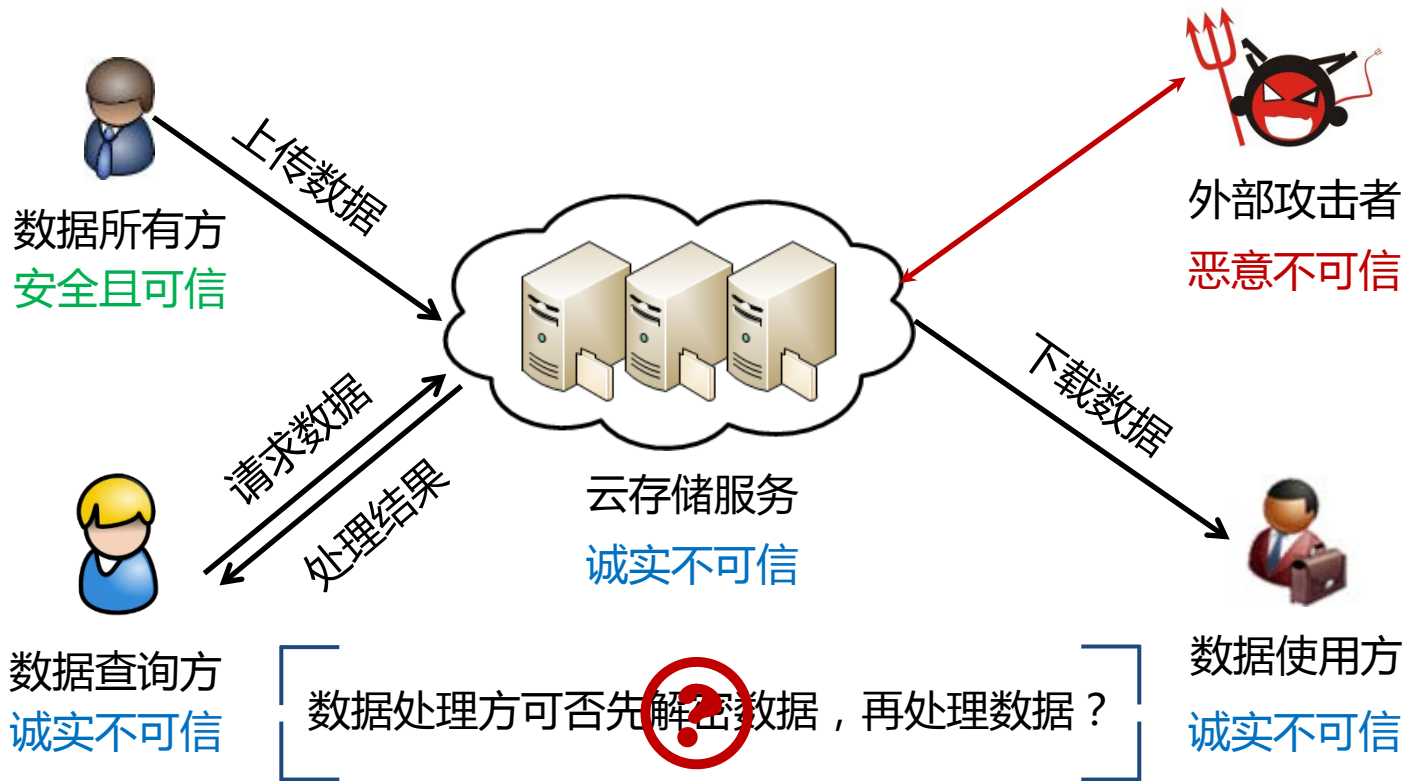
4 隐私保护数据发布

5 隐私保护统计数据发布

6 总结与展望

3 加密数据查询体系架构

在一般云存储体系架构中增加**数据查询方**，可对数据进行检索、计算等查询





数据库安全

目录

Contents

3.1 保序加密

3.2 同态加密

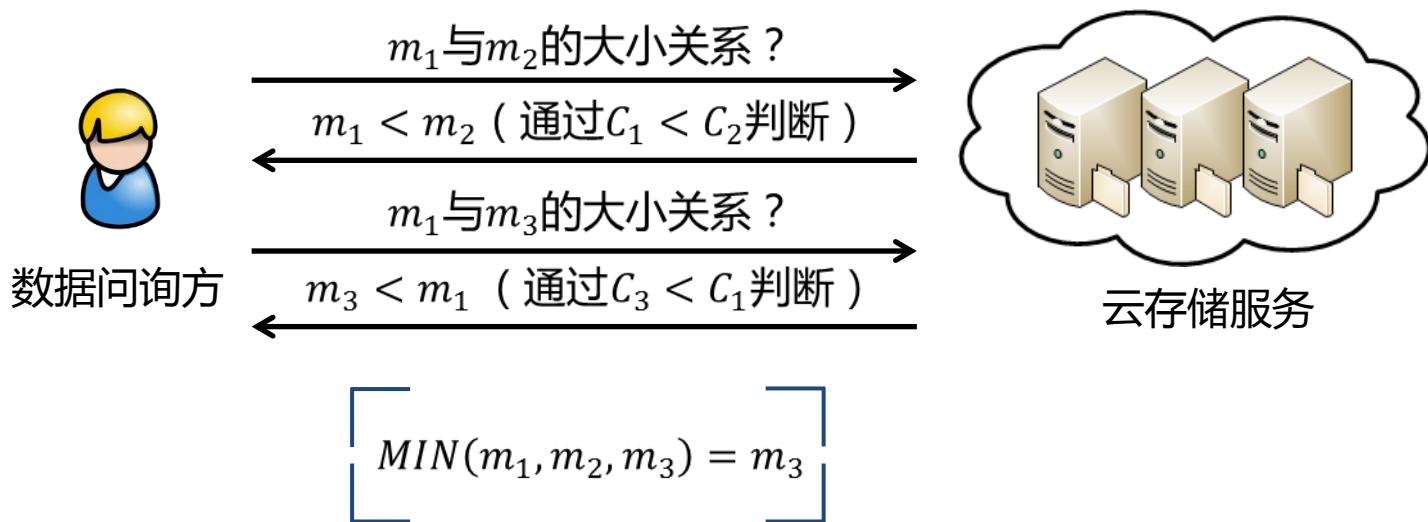
3.3 可搜索加密

3.4 实例：CryptoDB

3.1 保序加密 (Order-Preserving Encryption , OPE)

- **功能**：不解密数据的条件下，可通过加密结果直接判断数据的大小关系
- **原理**： $C_i = OPE_K(m_i)$, $C_j = OPE_K(m_j)$, $C_i < C_j \rightarrow m_i < m_j$
- **扩展**：应用OPE，可实现ORDER、BY、MIN、MAX、SORT等操作

实例：应用OPE实现3个未知数据 m_1, m_2, m_3 的MIN操作



3.2 同态加密 (Homomorphic Encryption , HE)

- **功能**：不解密数据的条件下，允许直接对加密结果进行代数操作
- **原理**： $HE_K(m_i) + HE_K(m_j) = HE_K(m_i + m_j)$
 $HE_K(m_i) \times HE_K(m_j) = HE_K(m_i \times m_j)$
- **扩展**：应用HE可在不解密的条件下实现数据处理，HE为云计算安全热点

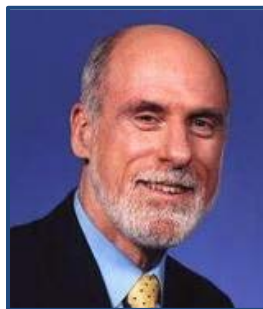
同态加密实例：很多加密算法允许直接对加密结果进行一部分代数操作

$$RSA_e(m) = m^e \bmod N$$

$$RSA_e(m_i) \times RSA_e(m_j) = m_i^e m_j^e \bmod N = (m_i m_j)^e \bmod N = RSA_e(m_i m_j)$$



Ron Rivest



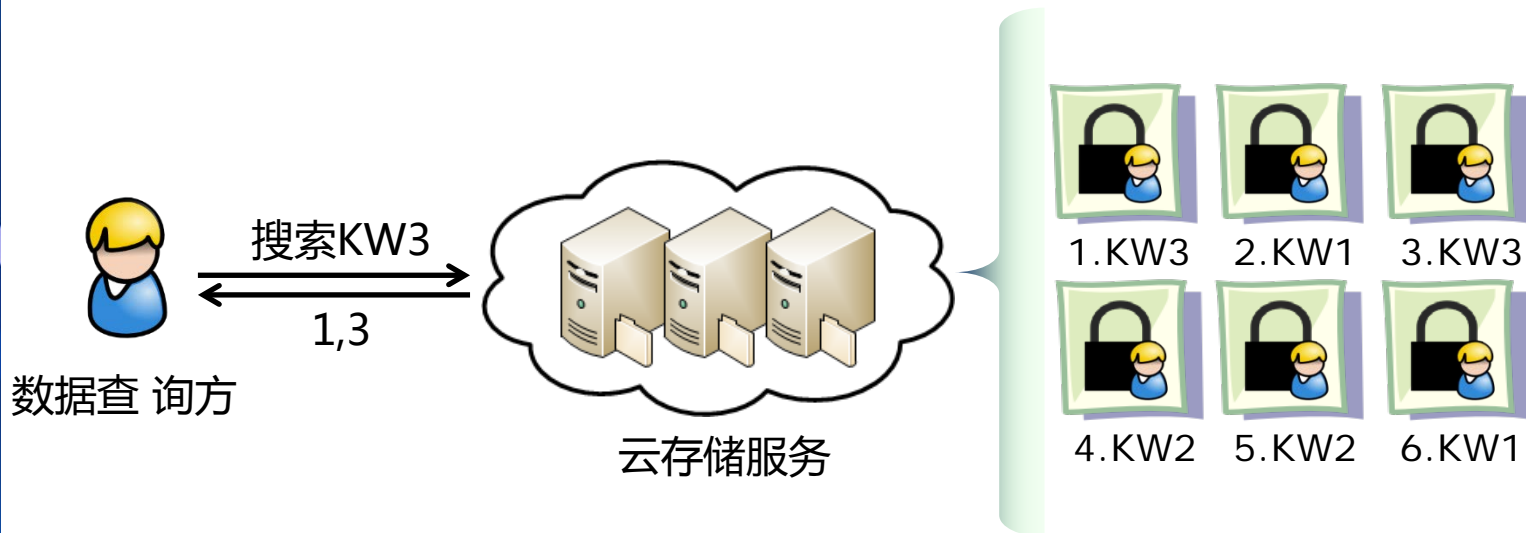
Adi Shamir



Leonard Adleman

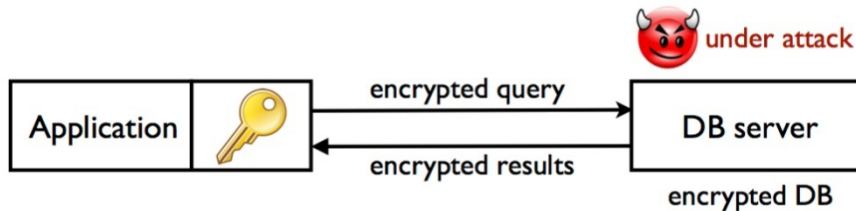
3.3 可搜索加密 (Searchable Encryption , SE)

- **功能**：不解密数据的条件下，允许直接对加密结果进行关键字或范围搜索
- **原理**：为每一个加密结果增加索引信息
数据使用方可以使用特殊的方法验证等式，实现搜索的功能
- **扩展**：综合使用OPE、HE和SE，可实现对加密数据的SQL查询



3.4 实例：CryptoDB

- 简介：麻省理工学院（MIT）设计并实现的密码学数据库
- 链接：<http://css.csail.mit.edu/cryptodb>
- 功能：数据库中的所有数据加密存储，允许第三方应用SQL语句进行查询
- 特性：首次实现密文数据SQL查询功能，大约只增加26%的计算开销
- 算法：综合使用数据加密、保序加密、同态加密、可搜索加密等方案



```
mysql> select * from table_YYAXXURGXH;
+-----+-----+-----+
| CKEWNNKTJV0DET | WIWHTQZBQ00PE | ISKNOMNOYS0AGG |
+-----+-----+-----+
| 12350108222818996780 | 14614281758989903640 | ;|L100|e0b(T 5|0-0  
(000?0;000[00f0000]0+0 0H"050\0000F0bv0Ts000400y0k000P02m000|000"  
00%00000'0<t4m00|0010 0p0 00c)0000c00000 0?mk00U0qi050|0nc0|000|00"  
| 15753844592636354766 | 16607196790268127689 | R P-01|000000|00f Ea|  
U|H=000 0|000h000f0u|000:00040|0S0z|00s00|0qz006C0  
y000U0|0b40e00|00c00|0y  
| 13411675538537145840 | 12454649889312668381 | 000pK^v0000000|0|0000  
00R000"0-0J 00_000(tm00)009T0M  
=f000g0000:0CR|000040og0+00g0+0z0000M|000(0(000MKhuv000c0F000(00000C|
```

谢 谢！

