**数据库加密技术**

1. **数据库加密的基本要求**
   1. **数据库加密的必要性**
   2. **基本要求**
   3. **数据库对加密算法的要求**
   4. **数据库加密后数据库功能受到的限制**
2. **数据库加密的实现机制**
   1. **DBMS提供加密功能——优点和缺点**
   2. **库外加密——优点和缺点**

**HSM**

* 1. **对比**

1. **关键影响因素**
   1. **加密粒度的选择**
   2. **加密算法**
2. **序列密码体制**
3. **分组密码体制**
4. **公开密钥体制**
5. PGP系统(Pretty Good Privacy)是目前世界上最好的一种混合密码系统，它结合了公钥算法和单钥算法的优点。

Phil zimmermann

* 1. **数据库加密系统对数据库密码的要求**
  2. **密钥管理**
  3. **数据库加密的局限性**
  4. **密文数据的查询**

1. **攻击加密数据库的方法**
   1. **获取密钥**
   2. **对比明密文攻击**
   3. **字典式攻击**
   4. **统计攻击**
2. **数据库加密技术的问题**
   1. **如何直接在字符型密文数据上执行带LIKE的子句**
   2. **如何直接在密文数据上执行范围查询**
   3. **密文数据的排序、分组**
   4. **密文索引的管理**
   5. **加密数据库的完整性问题**
   6. **SQL语言中的内部函数将对加密数据失去作用**
3. **数据库加密技术 ——目前的解决方法**

**6.1 缩小解密范围的方法——应用于DSP环境(数据服务提供者模型)**

**(1)关系加密和存储 ——可以使用任意的加密算法**

**(a)分区功能**

**(b) 识别函数**

**(c) 映射函数**

**(d) 存储加密数据**

**(e) 解密函数**

**(2)映射查询条件Mapcond**