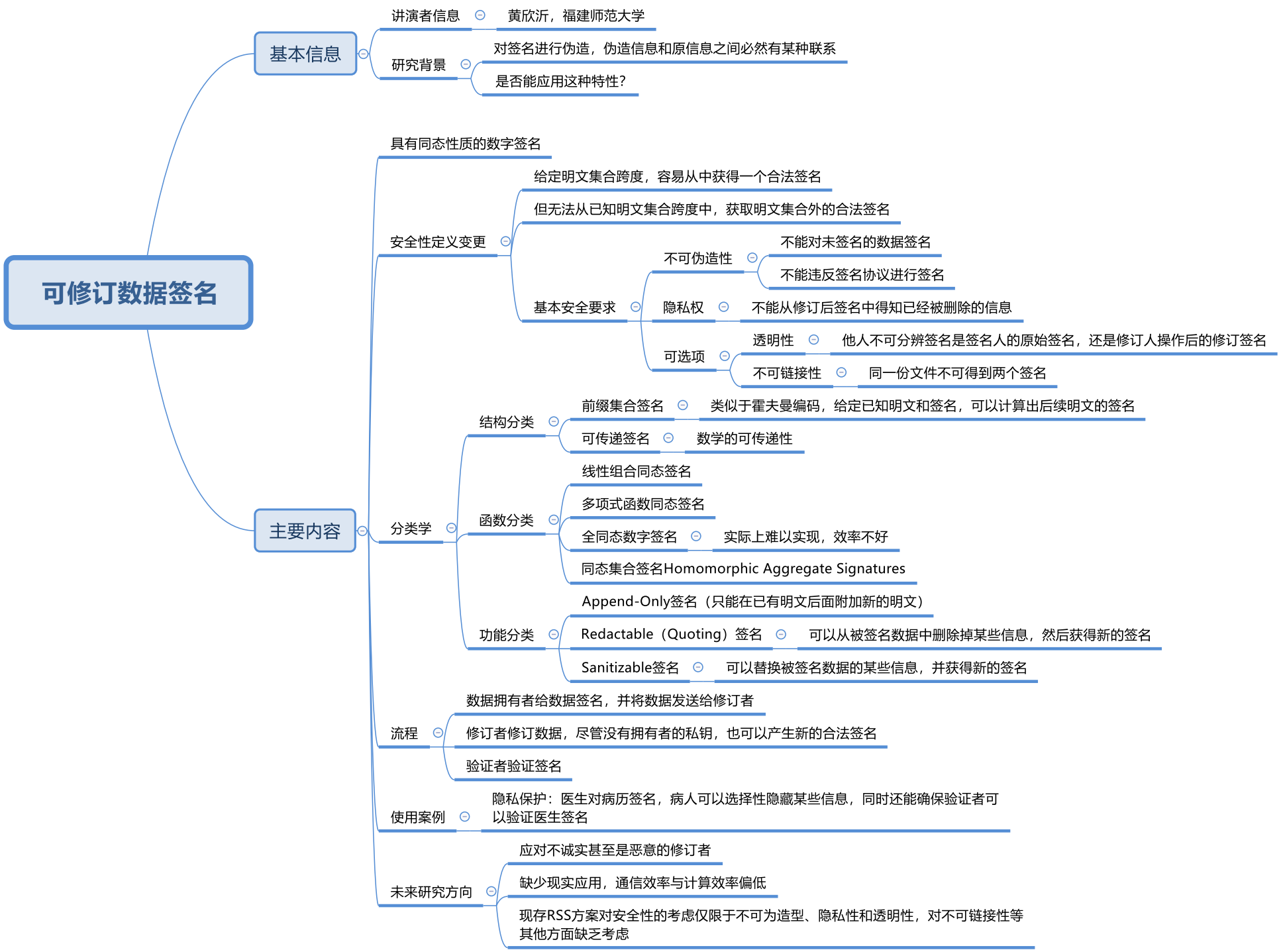
可修订数据签名
基本信息
讲演者信息
黄欣沂，福建师范大学
研究背景
对签名进行伪造，伪造信息和原信息之间必然有某种联系
是否能应用这种特性?
主要内容
具有同态性质的数字签名
安全性定义变更
给定明文集合跨度，容易从中获得一个合法签名
但无法从已知明文集合跨度中，获取明文集合外的合法签名
基本安全要求
不可伪造性
不能对未签名的数据签名
不能违反签名协议进行签名
隐私权
不能从修订后签名中得知已经被删除的信息
可选项
透明性
他人不可分辨签名是签名人的原始签名，还是修订人操作后的修订签名
不可链接性
同一份文件不可得到两个签名
分类学
结构分类
前缀集合签名
类似于霍夫曼编码，给定已知明文和签名，可以计算出后续明文的签名
可传递签名
数学的可传递性
函数分类
线性组合同态签名
多项式函数同态签名
全同态数字签名
实际上难以实现，效率不好
同态集合签名Homomorphic Aggregate Signatures
功能分类
Append-Only签名（只能在已有明文后面附加新的明文）
Redactable（Quoting）签名
可以从被签名数据中删除掉某些信息，然后获得新的签名
Sanitizable签名
可以替换被签名数据的某些信息，并获得新的签名
流程
数据拥有者给数据签名，并将数据发送给修订者
修订者修订数据，尽管没有拥有者的私钥，也可以产生新的合法签名
验证者验证签名
使用案例
隐私保护：医生对病历签名，病人可以选择性隐藏某些信息，同时还能确保验证者可以验证医生签名
未来研究方向
应对不诚实甚至是恶意的修订者
缺少现实应用，通信效率与计算效率偏低
现存RSS方案对安全性的考虑仅限于不可为造型、隐私性和透明性，对不可链接性等其他方面缺乏考虑