各位老师下午好，我叫王智坚，是信息与计算科学专业。我的毕业论文题目是《具有隐私保护的分布式统计》。

我论文的主要研究内容是，在分布式统计中，多方的数据提供者提供数据到计算服务商中，此时服务商若是拿到了没有加密过的数据，并且这些数据对于数据提供者来说是隐私数据的话，那么数据提供者的数据隐私得不到保护，这时发生了数据泄露，这是不好的。所以，若是在发送数据给计算服务商前，将数据进行加密之后再发送给计算服务商，服务商根据加密后的数据接着计算，将得到的结果返回数据提供商，数据提供商接着对结果解密，此时就能使得数据得到保护。

大致的研究框架分为三个模式，一对一模式，一个数据提供者，一个计算服务商，发送加密数据，结果对返回的结果解密就可以了。对于同态加密的方法，采用的是《支持同态算术运算的数据加密方案算法研究》中的“CESIL方案”，这个加密方法属于对称加密，即使运算过后，密文长度仍然不变，不会增加数据提供者接收密文结果数据时的通信开销。

第二个是，一个数据提供者，多个计算服务商。这种情况是数据提供者将自己的数据分为多份，发送给多个计算服务商。加密方法还是刚才提的“CESIL方案”，而对于数据的分发，采用文献《多租赁用户模型下有效安全外包计算》下的“安全的外包计算协议”，将数据x分为x1,x2,x3…xn分别给对应的计算服务商，接着将结果返回给数据提供者，数据提供者将结果整合，得到真正想要的结果。

第三个是，多个数据提供者，一个计算服务商。这种情况例如统计一个地域的环境，多个人手中有不同的数据，但是又不愿意相互共享，都是自己的隐私数据，而此时计算的话就可以引用文献《基于云计算服务的安全多方计算》中的“TFHE方案”，此方案在半恶意模型下安全，且各数据提供商得到真正的结果仅需要执行于TFHE相关的计算，而真正的计算任务则在计算服务商里进行。因此对各个数据提供者来说计算量不是很大。