课题二前端设计（初稿）

本篇文档主要讲述课题二对于算法前端展示的一些初步设想，用于提供给课题五作方案实现的可行性分析。 初稿主要涵盖已有的密码学部分的实现，神经网络部分将在后续补充。

密码学前端设计

密码学部分的前端展示主要需要达成算法的分解，部署和映射这样的目标

因此以下将按照这三个目标分开叙述课题二对密码学前端部分的设想。

密码学部分的优化实现，主要是将巨量多个独立的输入，按照负载比例分成不同的任务组，在不同的核组上运行。

因此算法的分解部分，可以将输入用一个大的矩形表示，在矩形内部用多个长条形表示不同的独立输入。 将整个大输入矩阵用一条线连到编译器，加上一个晶圆信息的输入，与一个表示可执行文件的矩形相连接。组成第一部分的分解解析部分，同时也可以作为编译部分的展示。

可执行文件分为两部分，一部分是提供给 GPU 运行的 PTX 文件，另一部分是 CPU 运行的计算部分和主控部分。 可以将他们用一个矩形划为一个主体，加上两个矩形分为不同的子部分，并与晶圆部分用线相连，代表算法的部署。

如上面分解部分所描述，最终各输入会通过负载比例分别加载到不同的核组上，因此映射部分的表示目前构思是 将不同的数据分区块连接到代表晶圆的矩形上。

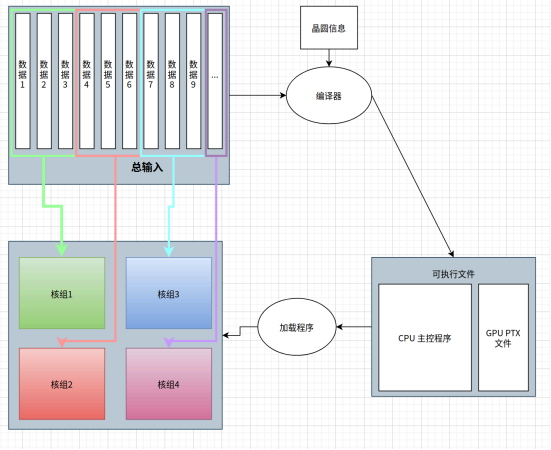

图 1　对上述设计的简单示意图