通过Intel SGX，应用程序可以在可信执行环境中执行代码并保护机密信息，使其抵御恶意软件的攻击，即便在应用程序、OS和BIOS都不可信的情况下也是如此，哪怕攻击者获取了整个平台的控制权，应用程序的机密信息依然可以收到保护，以便让开发者直接控制应用程序的安全性。

为了保护机密信息，Intel SGX在内存中划定了名为安全区（enclave）的隔离区域，用来存放代码和数据，这些不可寻址的分页内存是从系统的物理RAM中保留的，并且经过了加密。Enclave是受保护的内存区域，应用程序可以在里面处理它的机密数据，不必担心泄露它们。Intel SGX应用程序由两部分构建——可信部分和不可信部分。

当应用程序需要处理机密时，它会创建一个位于可信内存的enclave，然后调用可信函数，它是由应用开发者创建的、专门在enclave内执行的函数，一旦这个函数被调用，应用程序就会在可信区域执行并明文访问enclave中的代码和数据，除此之外，任何其他试图从enclave外访问enclave内存的行为都会被处理器拒绝，即使是系统特权用户的行为。这种机制使得安全区内的机密不被泄露。当可信函数执行完毕后，安全区内的数据依然保留在可信内存中，而应用程序返回到不可信区域继续执行，并且失去了对可信内存的访问权限。

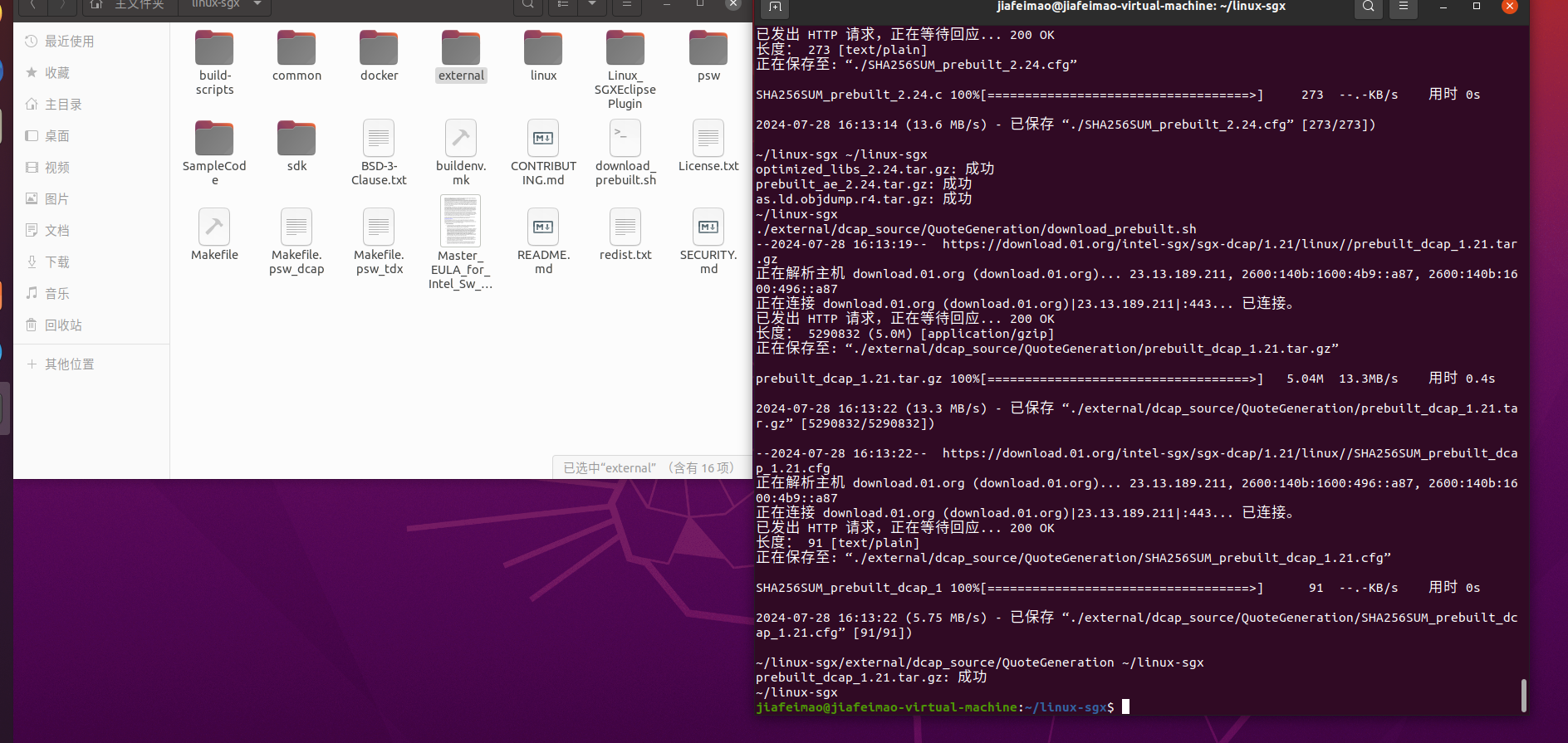
开发手册：<https://download.01.org/intel-sgx/latest/linux-latest/docs/Intel_SGX_SW_Installation_Guide_for_Linux.pdf>

虚拟机Ubuntu 20.04环境下安装

安装linux SGX开发环境：

1. Intel® SGX Driver √
2. Intel® SGX Software Development Kit (SDK)

make preparation结果：（终于成功了，老泪纵横）



1. Intel® SGX Platform Software (PSW) for Linux\* OS
2. Intel® SGX Data Center Attestation Primitives (DCAP) for Linux\* OS