文章链接：<https://zhuanlan.zhihu.com/p/46477111>

代码连接：<https://github.com/kunxian-xia/sudoku-zk-snarks>

代码编译

源码分析

一．参考资料

**1.《零知识证明 - libsnark源代码分析》**<https://zhuanlan.zhihu.com/p/78683739>

**2.《Zksnark--终极原理》（一共4篇，熟悉zksnark的不用看）**

<https://blog.csdn.net/guoyihaoguoyihao/article/details/103056081>

1. 个人源码分析

《main.cpp》

在main函数中，调用了alt\_bn128椭圆曲线，并且根据椭圆曲线、数独约束和证明系统生成了对应的公司钥对（keyPair）。接着将keyPair传入test\_completeness函数，该函数提供了一个4\*4的数独的题和解，主要流程是对这个解进行零知识证明，并且验证证明结果。

《soduku\_snark.cpp》

这里面提供了3个零知识证明关键步骤的方法，分别为generate\_keypair、generate\_proof和verify\_proof方法。