§5.4 零知识证明

零知识证明是这样一种技术，即当示证者P掌握某些秘密信息，P设法向验证者V证明自己掌握这些信息，验证者V可以验证P是否真的掌握这些秘密信息，但同时P又不想让V也知道那些信息。该技术比传统的密码技术更安全并且使用更少的处理资源。但是它需要更复杂的数据交换协议，需要更多的数据传输，因此会消耗大量通信资源。

一般来说，被示证者P掌握的秘密信息可以是某些长期没有解决的猜想问题。如大整数因式分解和求解离散对数问题等，还可以是一些单向函数等。但信息的本质是可以验证的，即可通过具体的步骤来检测它的正确性。

§5.4 零知识证明

零知识证明需满足的条件：

（1）示证者几乎不可能欺骗验证者，

若P知道证明，则可使V几乎确信P知道证明；

若P不知道证明，则他使V相信他知道证明的概率近于零。

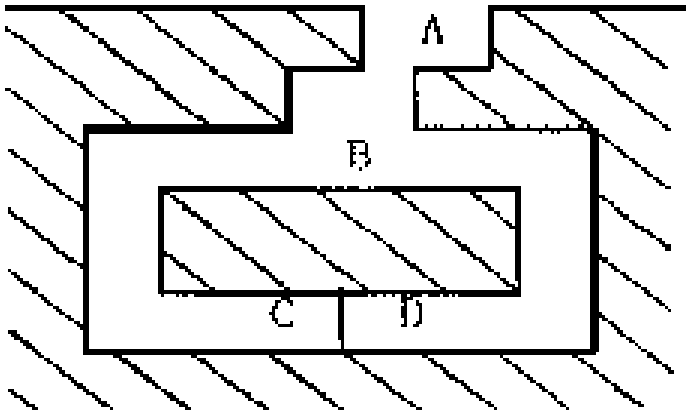
（2）验证者几乎不可能得到证明的信息，特别是他不可能向其他人出示此证明。

（3）验证者从示证者那里得不到任何有关证明的知识。

§5.4 零知识证明

例1：洞穴问题（见图）。

设P知道咒语，可打开C和D之间的秘密门，不知道者都将走入死胡同中。现在看看P如何向V出示证明使V相信他知道这个秘密，但又不告诉V有关咒语：



（1）V站在A点；

（2）P进入洞中任意一点C或D；

（3）当P进洞之后，V走到B点；

（4）V叫P：“从左边出来”或“从右边出来”；

（5）P按要求实现；

（6）P和V重复执行（1）至（5）共n次。

§5.4 零知识证明

例2：Hamilton回路零知识证明协议。

（1）P对图G作一随机置换，得一个与其同构的新图G_1，P很容易知道G_1的Hamilton回路；

（2）P将图G_1发给V；

（3）V随机的要求P完成：“证明图G和G_1同构”或“指出图G_1的一个Hamilton回路”；

（4） P按要求实现：“证明图G和G_1同构，但不指出图G和G_1的Hamilton回路”或“指出图G_1的一个Hamilton回路，但不指出图G和G_1同构”；

（5）P和V重复执行（1）至（4）共n次。