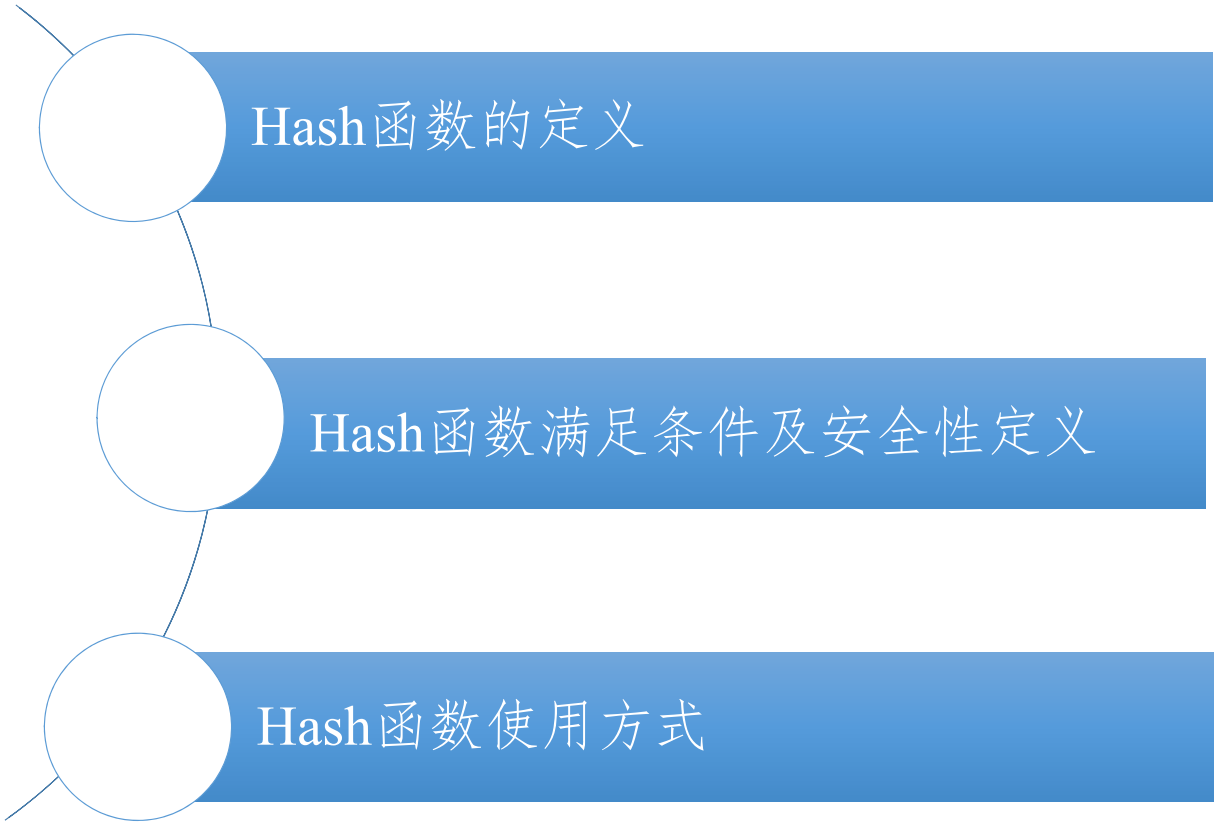
第41讲 Hash函数

廖永建

信息与软件工程学院

liaoyj@uestc.edu.cn

第41讲 Hash函数



Hash函数的定义

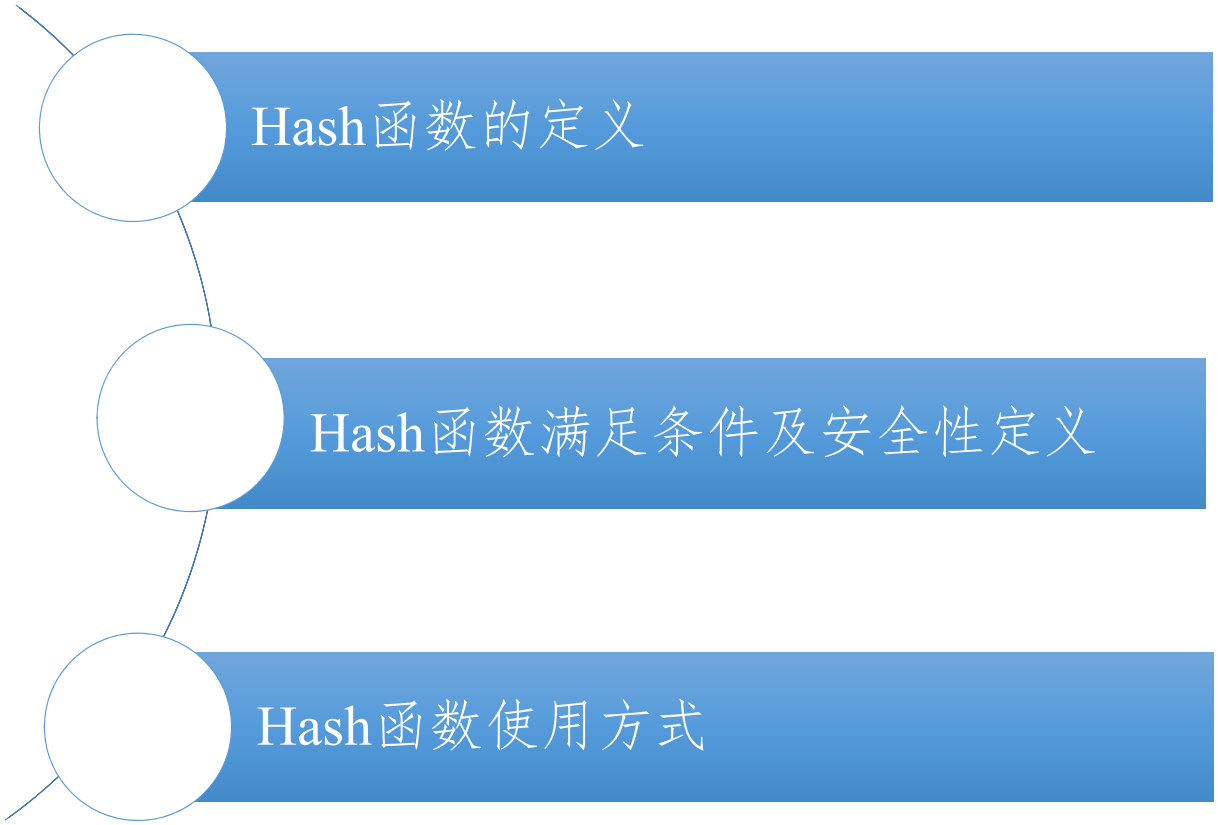
- Hash函数的定义
  - 将任意长的消息M映射为较短的、固定长度的一个值H(M)。
  - Hash函数也称为哈希函数、散列函数、压缩函数、杂凑函数、指纹函数等。其函数值H(M)为哈希值、散列值、杂凑码、指纹、消息摘要等。
  - Hash函数H一般是公开的。

例1

M 是一个长消息，设$M=(M_1, M_2, \cdots\cdots, M_k)$，其中$M_i$为$l$长的比特串，定义函数$H$如下：

- $H(M) = M_1 \oplus M_2 \oplus \cdots\cdots \oplus M_k$

第41讲 Hash函数



Hash函数满足条件

- Hash函数的目的是为需认证的数据产生一个“指纹”，Hash函数应满足以下条件：
  - Hash函数函数的输入可以是任意长
  - Hash函数函数的输出是固定长
  - 易于在软件和硬件实现

Hash函数满足的安全条件

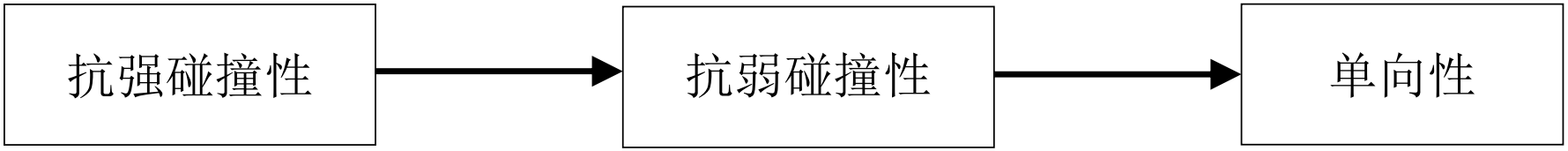
- 同时，Hash函数为了实现安全认证，需要满足如下安全条件：
  - 单向性：已知x，求H(x)较为容易；但是，已知h，求使得H(x)=h的x在计算上是不可行的。
  - 抗弱碰撞性：已知x，找出y(y≠x)使得H(y)=H(x)在计算上是不可行的。
  - 抗强碰撞性：找出任意两个不同的输入x、y，使得H(y)=H(x)在计算上是不可行的。

例1（续）

M 是一个长消息，设$M=(M_1, M_2, \cdots\cdots, M_k)$，其中$M_i$为$l$长的比特串，定义函数$H$如下：

- $H(M) = M_1 \oplus M_2 \oplus \cdots\cdots \oplus M_k$

3个安全性的关系

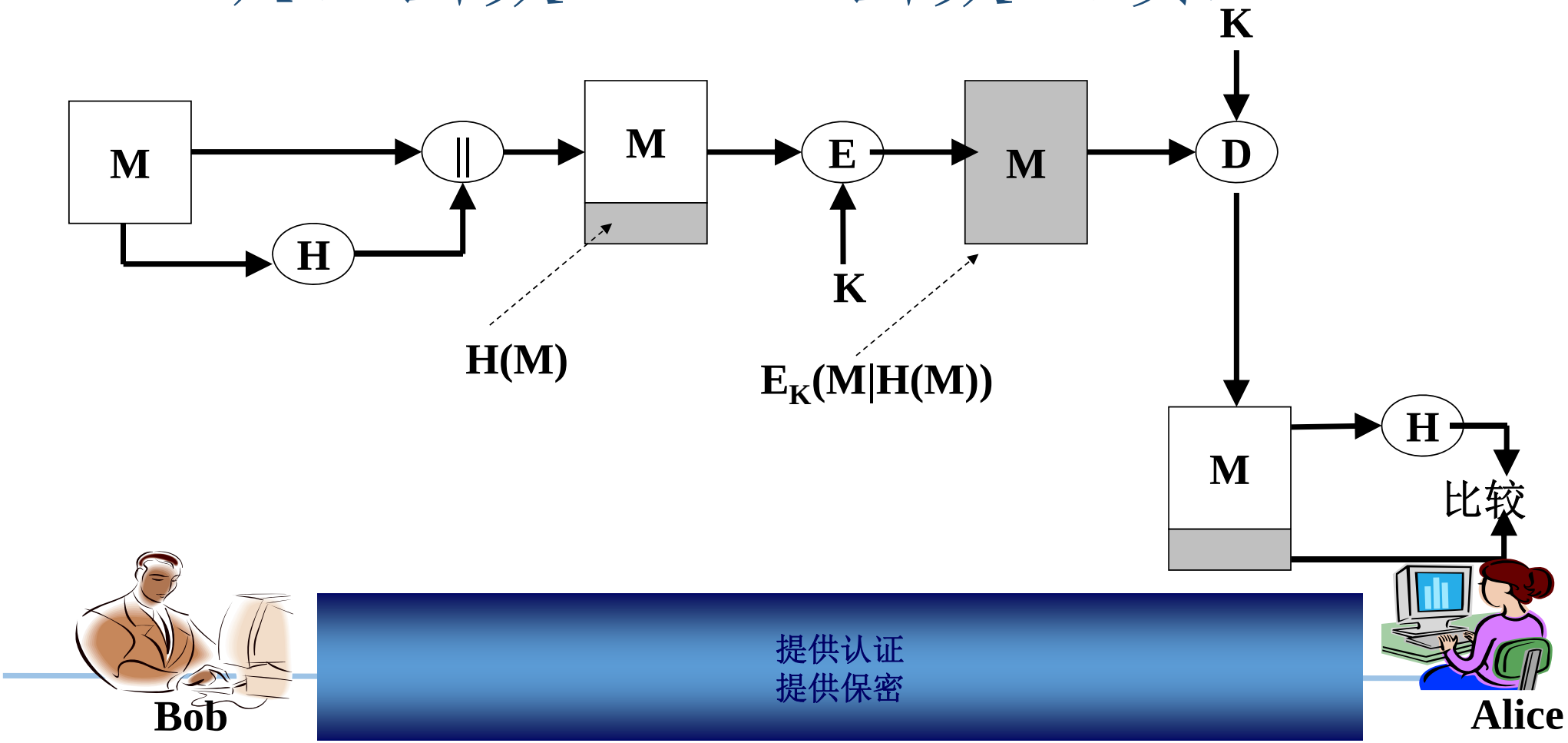


第41讲 Hash函数

- Hash函数的定义
- Hash函数满足条件及安全性定义
- Hash函数使用方式

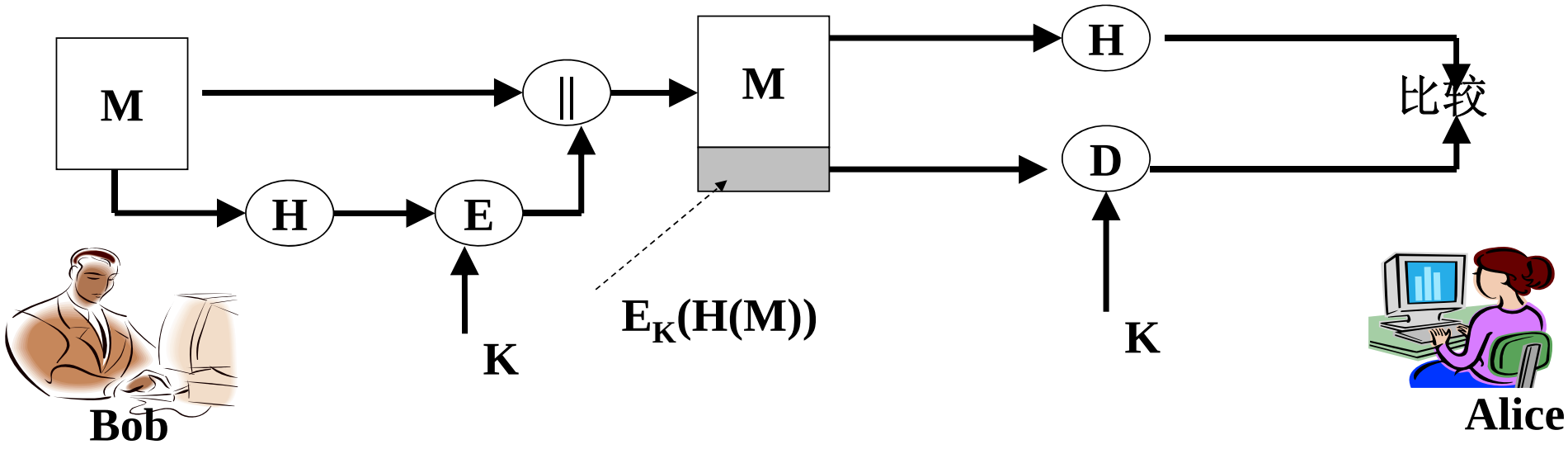
认证函数：Hash函数-基本用法（a）

认证函数：Hash函数（续）



认证函数：Hash函数（续）

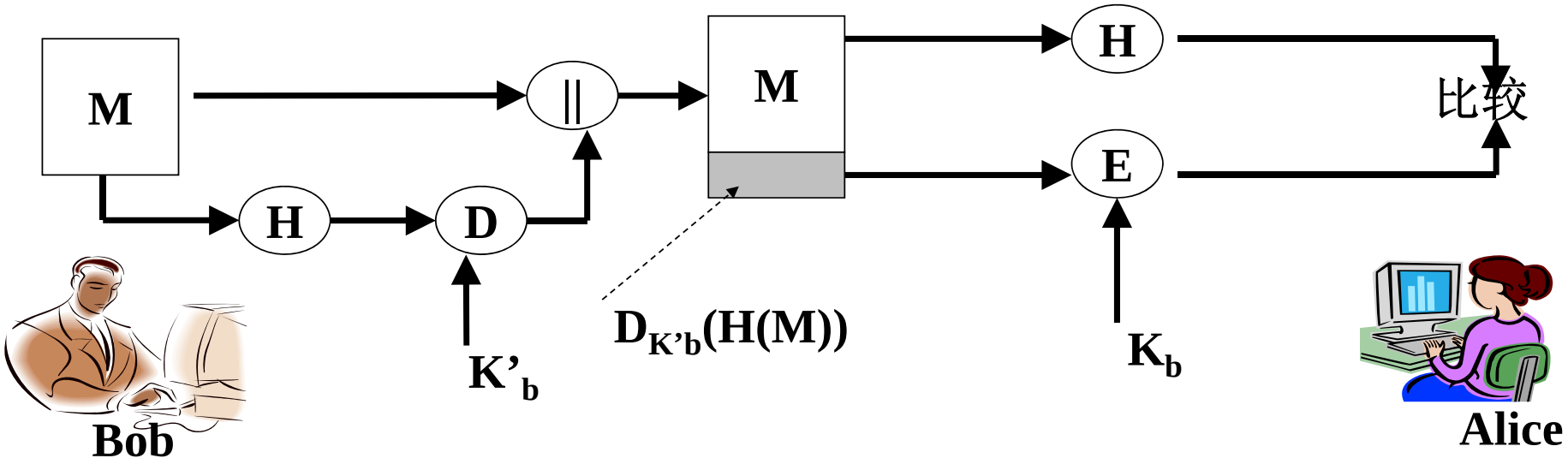
哈希函数的基本用法（b）



提供认证

认证函数：Hash函数（续）

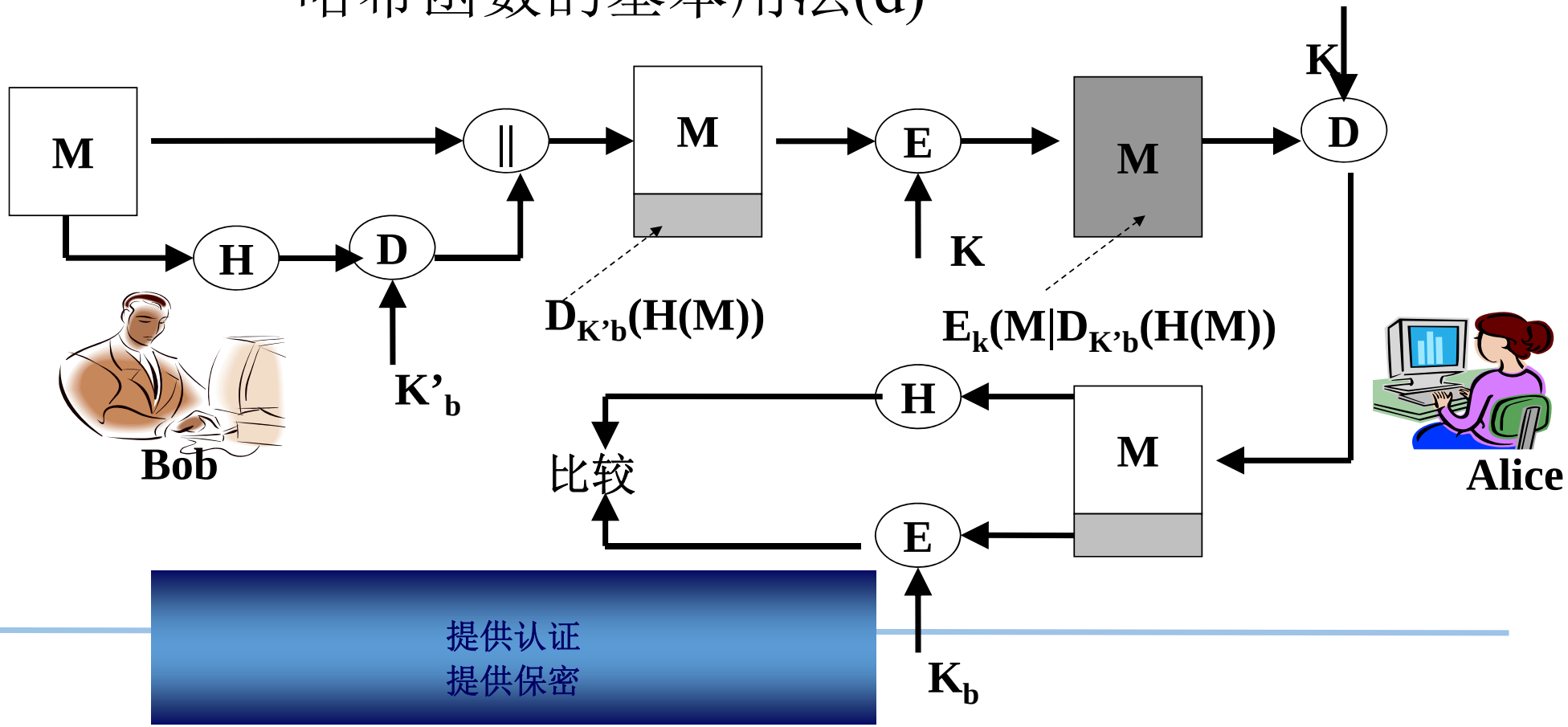
哈希函数的基本用法（c）



提供认证

认证函数：Hash函数（续）

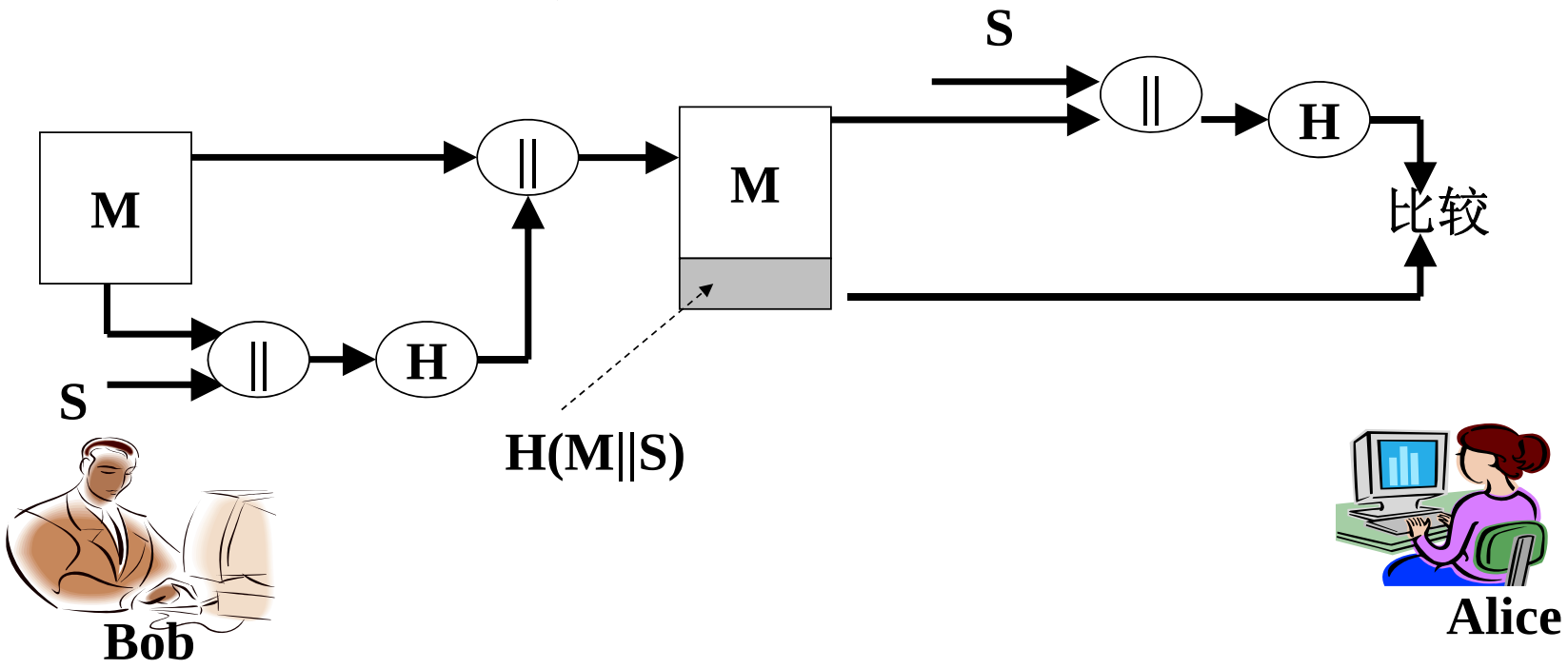
哈希函数的基本用法(d)



提供认证
提供保密

认证函数：Hash函数（续）

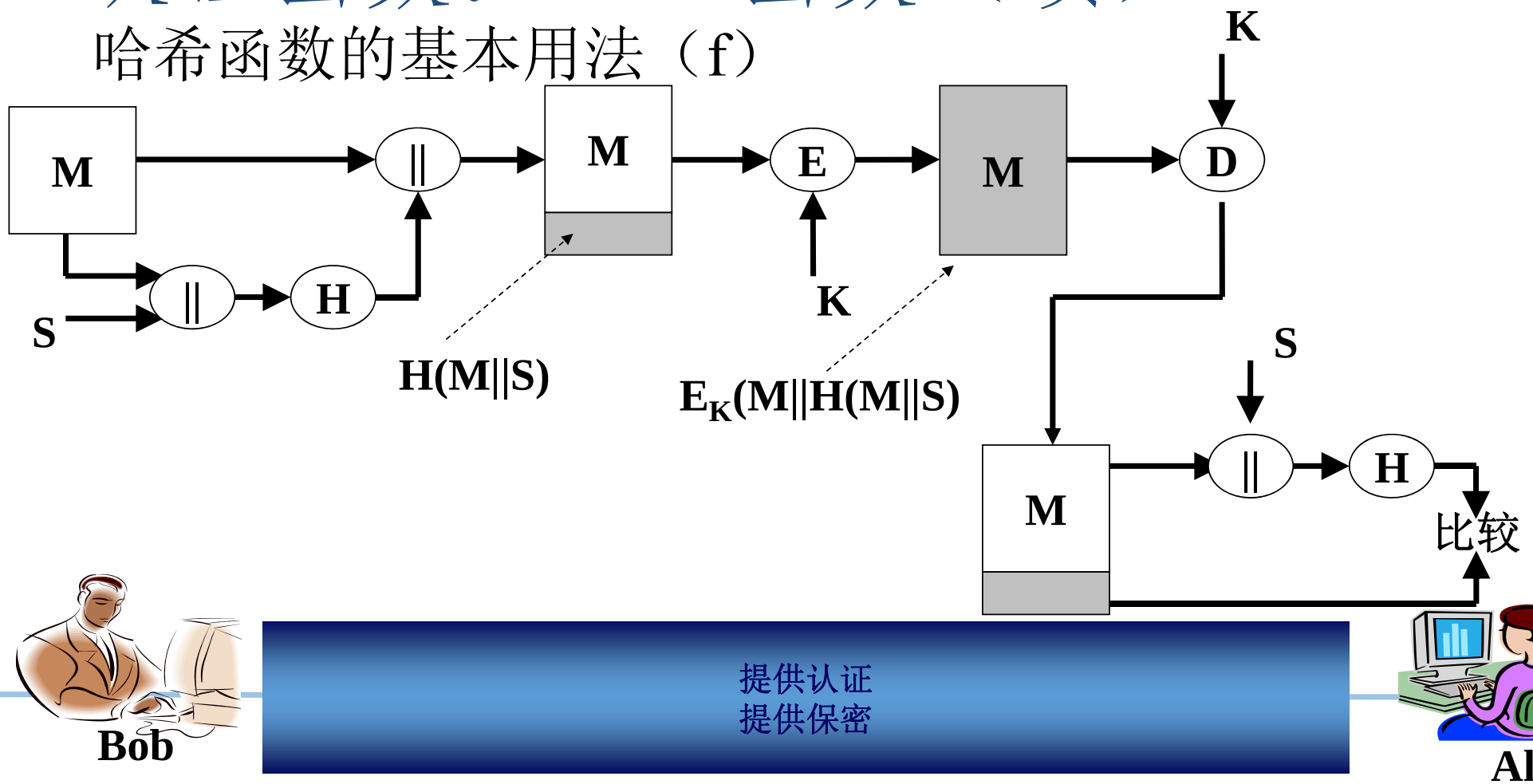
哈希函数的基本用法（e）



提供认证

认证函数：Hash函数（续）

哈希函数的基本用法（f）



谢谢