- 1　密码协议概述
- 2　不经意传输协议
- 3　密钥认证协议
- 4　比特承诺协议
- 5　零知识证明与身份识别协议
- 6　电子投票协议
- 7　电子拍卖协议
- 8　公平交换协议

不经意传输协议

- 设A有一个秘密，想以1/2的概率传递给B，即B有50%的机会收到这个秘密，另外50%的机会什么也没有收到，协议执行完后，B知道自己是否收到了这个秘密，但A却不知B是否收到了这个秘密。这种协议就称为不经意传输协议。

- 不经意传输协议分类
  - 基于大数分解问题的不经意传输协议
  - 基于离散对数问题的不经意传输协议
  - “多传一”的不经意传输协议

- **基于大数分解问题的不经意传输协议**

  设A想通过不经意传输协议传递给B的秘密是整数n（为两个大素数之积）的因数分解。这个问题具有普遍意义，因为任何秘密都可通过RSA加密，得到n的因数分解就可得到这个秘密。

- 协议基于如下事实：已知某数在模n下两个不同的平方根，就可分解n。

- 协议如下：

① B随机选一数x，将$x^2 \bmod n$发送给A。

② A（掌握$n = pq$的分解）计算$x^2 \bmod n$的四个平方根$\pm x$和$\pm y$，并将其中之一发送给B。由于A只知道$x^2 \bmod n$，并不知道四个平方根中哪一个是B 选的x。

③ B检查第②步收到的数是否与$\pm x$在模n下同余，如果是，则B没有得到任何新信息；否则B就掌握了$x^2 \bmod n$的两个不同的平方根，从而能够分解n。而A却不知究竟是哪种情况。显然，B得到n的分解的概率是1/2。

- 基于离散对数问题的不经意传输协议

  设系统中所有用户都知道一个大素数p、$GF(p)-\{0\}$的生成元g和另一大素数c，但无人知道c的离散对数。

  假定计算离散对数是不可行的，因此从$g^x \bmod p$和$g^y \bmod p$

  无法计算$g^{xy} \bmod p$。

  - **协议中所有**运算都在$GF(p)$中进行

B按如下方式产生公开的加密密钥和秘密的解密密钥：

- 随机选取一个比特i和一个数$x(0 \le x \le p-2)$,
- 计算：$y_i = g^x$，　$y_{1-i} = c(g^x)^{-1}$,
- 以$(y0, y1)$作为公开的加密密钥，以(i, x)作为秘密解密密钥。
- 由于B不知道c的离散对数，所以他知道y_0和y_1两者其中一个的离散对数，而A无法知道y_0和y_1中哪个离散对数是B已知的。
- A可通过方程 $y_0 y_1 = c$ 来检查B的公开加密密钥是否正确。

- 协议如下：

①A在0到$p-2$之间随机取两个整数k_0，k_1。对$j=0,1$，计算$c_j=g^{k_j}$，$d_j=y_j^{k_j}$，$m_j=s_j\oplus d_j$。将c_0，c_1，m_0，m_1发送给B。

②B用自己的秘密解密密钥计算$c_i^x=g^{k_i x}=y_i^{k_i}=c_i$，$s_i=m_i\oplus d_i$

由于B不知道y_{1-i}的离散对数，所以无法得到d_{1-i}和s_{1-i}。

注：本协议相当于“二传一”不经意传输。若其中一个为有效秘密一个为空，则成为前一种不经意传输。

- “多传一”的不经意传输协议

  设A有多个秘密，想将其中一个传递给B，使得只有B知道A传递的是哪个秘密。设A的秘密是$s_1, s_2, \ldots, s_k$，每一秘密是一比特序列。

- 协议如下：

① A告诉B一个单向函数f，但对f^{-1}保密。

② 设B想得到秘密s_i，他在f的定义域内随机选取k个值$x_1, x_2, \ldots, x_k$，将k元组$(y_1, y_2, \ldots, y_k)$发送给A，其中

$$y_j = \begin{cases} x_j & j \neq i \\ f(x_j) & j = i \end{cases}$$

③ A计算 $z_j=f^{-1}(y_j)$ $(j=1,2,\ldots,k)$，并将$z_j \oplus s_j$ $(j=1,2,\ldots,k)$发送给B。

④ 由于 $z_i=f^{-1}(y_i)=f^{-1}(f(x_i))=x_i$，所以B知道$z_i$，因此可从$z_i \oplus s_i$获得$s_i$。

由于A不知 k 元组$(y_1, y_2, \ldots, y_k)$中哪个是$f(x_i)$，因此无法确定B得到的是哪个秘密。

然而如果B不遵守协议，他用 f 对多个x_j求得 $f(x_j)$，就可获得多个秘密。因此总假定这种“多传一”协议中所有用户都遵守协议。

- 1　密码协议概述
- 2　不经意传输协议
- 3　密钥认证协议
- 4　比特承诺协议
- 5　零知识证明与身份识别协议
- 6　电子投票协议
- 7　电子拍卖协议
- 8　公平交换协议

电子拍卖协议

- 拍卖活动是电子商务中的一种基本活动，它是由拍卖群体决定价格及分配特殊现货的交易方式。一般情况下，拍卖企业接受委托，在规定的时间和地点，按照一定的规则和程序，由拍卖师主持，买卖双方之间产生一个合理的并参与各方都认可的价格，最后把商品卖给出价最高的竞买者。

- **电子拍卖的基本组成和现实生活中的拍卖是一样的，均由拍卖参与者、拍卖规则和仲裁机构组成。**

  - 拍卖参与者包括投标者、卖方和拍卖服务器。
  - 拍卖服务器像传统拍卖行的店，提供拍卖业务，是电子拍卖系统的关键部件。
  - 拍卖规则是指买卖双方认可和确定的拍卖和成交原则。
  - 仲裁机构负责解决买方之间、买卖双方之间以及他们和拍卖行之间的拍卖纠纷。仲裁机构是可信赖的第三方，只有在纠纷发生后，仲裁机构才介入。

电子拍卖规则

- 价格递增拍卖(英式拍卖)

首先拍卖行给出所拍卖商品的最低限价，然后经过多次竞价，其拍卖价逐次增加，直到只有一个竞买人竞价时为止，买受人就是最后一次竞买人，成交价就是买受人最后一次所竞价的价格。

- 价格递减拍卖(荷式拍卖)

拍卖行先给出所拍卖商品的最高标价， 然后经过多次竞价，拍卖价逐次增少，第一个竞价的人即为竞买人，成交价 就是其第一个竞价的价格。

- 密封式标价拍卖

所有竞买人把他们的竞标书密封(如加密)后送给拍卖行，拍卖行打开所有的竞标书以确定中拍卖价和买受人，拍卖价为竞标书中最高竞标的价格。

- 第二价位拍卖

竞标方式与密封式拍卖相同，竞标价格最高的竞标人为买受人，而拍卖价为次竞标价格。

电子拍卖规则的分析

- 英式拍卖花费的时间和通信代价都很高，而且会泄露有关投标者的信息。
- 荷兰式拍卖虽然不会泄露除中标者之外的其他投标者的任何信息，但时间代价也可能会很大。
- 密封式拍卖可在单轮通信中完成，但拍卖行一般会知道各投标者的出价，同时不支持商品的最优分配。
- 第二价位拍卖时间代价较小，但也可能不能保护投标者的隐私。

电子拍卖安全要求

- 匿名性：标价不能泄露投标者的身份。
- 可跟踪性：能追踪最后获胜的投标者。
- 不可冒充性：任何投标者不能被冒充。
- 不可伪造性：任何人不能伪造投标者的标价。
- 不可否认性：获胜者不能否认自己投的获胜标价。
- 公平性：合法的投标者在平等的方式参与投标活动。

电子拍卖安全要求（续）

- 公开验证：任何人都能验证投标者的合法性、标价的有效性以及公示获胜者的合理性。
- 不可链接性：同一投标者在多次拍卖投标中的标价不能被联系一起。
- 可链接性：在同一拍卖投标中，任何人能确定同一投标者的标价及标价次数。
- 一次注册：一次注册后，投标者可参加多次拍卖活动。
- 易撤销性：注册管理员能很容易撤销某一投标者。
- 高效性：投标和验证过程中的计算量和通信量满足实际需要。

电子拍卖系统基本组成

- 参与人员
- 布告栏
- 保密数据库

参与人员

注册管理者（RM）

- 负责注册过程并保存投标者的注册信息；
- 参与每次拍卖的密钥设置并在布告栏上无序地公布这次拍卖投标者使用的密钥；
- 在中标者公示阶段，在公告栏上公布中标者的特定信息。

拍卖管理者（AM）

- 在每次拍卖中，为每个投标者设置拍卖参数并在公告栏上无序地发布；
- 在中标者公示阶段，在公告栏上公布中标者的特定信息；
- 拥有公私钥对（x_A，y_A），其中$yA \equiv gxA \bmod p$。

投标者（B）

- 必须首先向RM申请注册才可参与拍卖；
- 必须使用每次拍卖设定参数参与拍卖活动；
- 拥有公私钥对（xi，yi），其中$yi \equiv gxi \bmod p$。

布告栏

- 注册布告栏(RM)
- 拍卖密钥布告栏(RM)
- 拍卖参数布告栏(AM)
- 标价公告栏(B)
- 中标者公告栏(RM和AM)

RM公布已注册投 标者的标识和公钥。

在每场拍卖时，RM为每个已注册投标者生成拍卖密钥并在本布告栏无序地公布。

在每场拍卖时，AM为每个已注册投标者生成拍卖参数并在本布告栏无序地公布。

投标者在本公告栏公布自己的标价，且只有比现有标价高的标价才能在本布告栏公示，任何人不能阻止有效的标价。

在中标者公示阶段，由RM和AM联合公布中标者的身份。

保密数据库

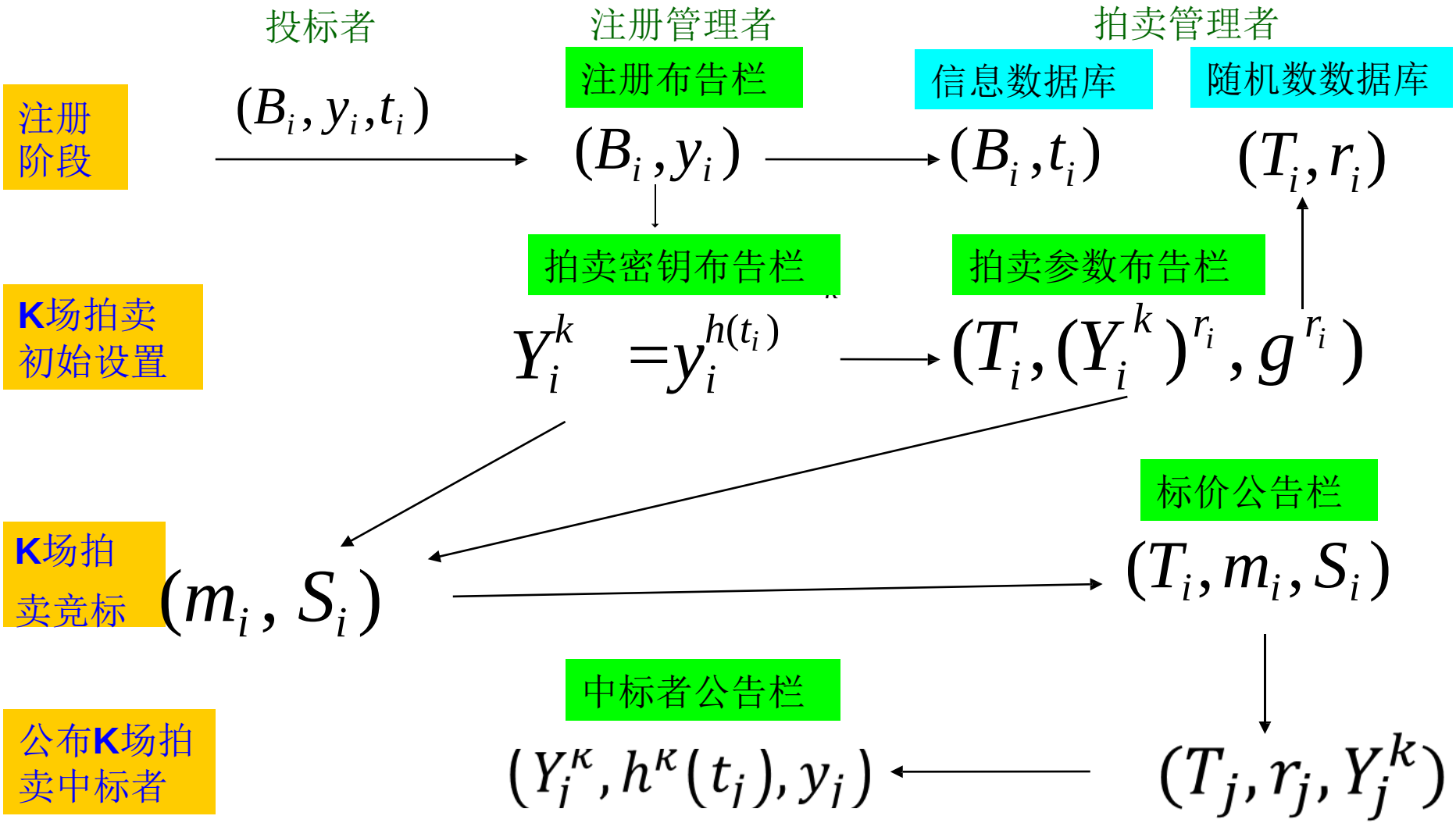
- 投标者信息数据库(RM)

RM为已注册的投标者保存秘密的用户信息。

- 随机数数据库(AM)

AM保存为每场拍卖产生拍卖参数的秘密随机数。

总流程图


投标者
注册管理者
拍卖管理者
注册阶段
(B_i, y_i, t_i)
注册布告栏
(B_i, y_i)
信息数据库
(B_i, t_i)
随机数数据库
(T_i, r_i)
拍卖密钥布告栏
$Y_i^k = y_i^{h(t_i)}$
拍卖参数布告栏
$(T_i, (Y_i^k)^{r_i}, g^{r_i})$
K场拍卖初始设置
K场拍卖竞标
(m_i, S_i)
标价公告栏
(T_i, m_i, S_i)
中标者公告栏
$(Y_i^\kappa, h^\kappa(t_i), y_i)$
(T_j, r_j, Y_j^k)
公布K场拍卖中标者

- 1　密码协议概述
- 2　不经意传输协议
- 3　密钥认证协议
- 4　比特承诺协议
- 5　零知识证明与身份识别协议
- 6　电子投票协议
- 7　电子拍卖协议
- 8　公平交换协议

公平交换协议的基本概念

- 公平交换协议的定义
- 公平交换协议的基本模型
- 公平交换协议的基本要求

公平交换协议定义

- 假设Alice想在Bob公司购买一张机票。Alice首先发出一个预订请求，Bob公司确认后向Alice发出一个通知。
- 问题：Alice发出了预订请求，但后来没有购买机票，Bob公司受损；另一方面，若Bob公司收到了预订请求，却将机票卖给了别人，那么Alice只好延期旅行。
- 如果只有一方诚实的执行协议，就无法保证双方的利益不受损失。即使Alice的请求和Bob公司的通知都具有不可否认性，也不能完全解决协议的公平性，这是因为双方的行为不具有同时性。若Alice首先发出一个不可否认请求，而Bob没有进行响应，于是，Alice就面临风险；如果她在别处预订，就有可能买到两张机票；如果不预订，则有可能面临没有机票的风险。

公平交换协议定义

- 当一个系统涉及到两个或者多个互不信任的主体，就要考虑满足所有主体的安全性。
  - 从主体利益的角度考虑，如果一个系统不会损害其中任何一个诚实主体的利益，那么该系统具有公平性。
  - 从交换的结果考虑，如果在交换结束后，要么每一方都得到了他所期待的信息或者物品，要么每一方都没有得到任何有意义的东西，我们也认为系统具有公平性。
- 需要存在相应的安全机制来保证交换顺利进行。这种安全机制就是公平交换协议。

公平交换协议的基本模型

- 假设desc ( )为交换商品的描述函数(对输入的任何一个交换商品，返回一个对该物品的描述)，P、Q为参与双方，他们的交换物品用i_P、i_Q表示，期望得到的对方交换物品描述为d_P、d_Q。
- 公平交换问题描述如下：
  - 交换之前P输入i_P、d_Q、Q，Q输入i_Q、d_P、P，代表P想用i_P跟Q交换描述为d_Q的交换物品，Q想用i_Q跟P交换描述为d_P的交换物品。交换之后P输出i_Q，Q输出i_P。

公平交换协议的基本模型

P　　Q

输入i_P、d_Q、Q　　输入i_Q、d_P、P

经过公平交换

输出i_Q，
其中$d_Q = desc(Q)$

输出i_P，
其中$d_P = desc(P)$

或者

取消　　取消

公平交换协议的基本要求

- 有效性：如果两个参与者行为正确，在不涉及第三方的情况下，仍能获得各自所需的东西。
- 秘密性：交换必须保护用户的隐私信息。
- 高效实用性：协议的效率要高，以保证实用性。
- 不可否认性：在进行有效的交换后，交换的任何一方都不能对他所传递和收到的信息进行否认。

公平交换协议的基本要求

- 公平性：在交换结束后，要么每一方都得到他所期待的物品(或服务)，要么每一方都没有得到任何有意义的东西。公平性又分为强公平性和弱公平性。
  - 强公平性：在协议的任何阶段，参与协议的任何诚实的主体都不处于劣势。交换结束后，参与交换的各方或者得到自己想要得到的东西，或者都没有得到任何有用的东西。
  - 弱公平性：在协议执行的某个阶段，即使诚实的主体处于某种程度的不公平，在以后的争论中，诚实的主体可以向仲裁者提供协议中的证据恢复公平性。

公平交换协议的基本要求

- 终止性：在协议执行的任何时间，每个参加者可以单方面中止协议而不破坏公平性。
- 第三方可验证性：发生纠纷时第三方可以进行仲裁，对不诚实的一方可以进行制裁。同时，如果第三方不诚实使得该协议对Alice不公平，则Alice可以向仲裁者证明第三方的不公正行为。
- 无滥用性：在多方公平交换模型中，参与交换的任意子集在协议的任何时刻，都无法向第三者证明他们有能力中止(或完成)协议。