数字签名

不可否认性

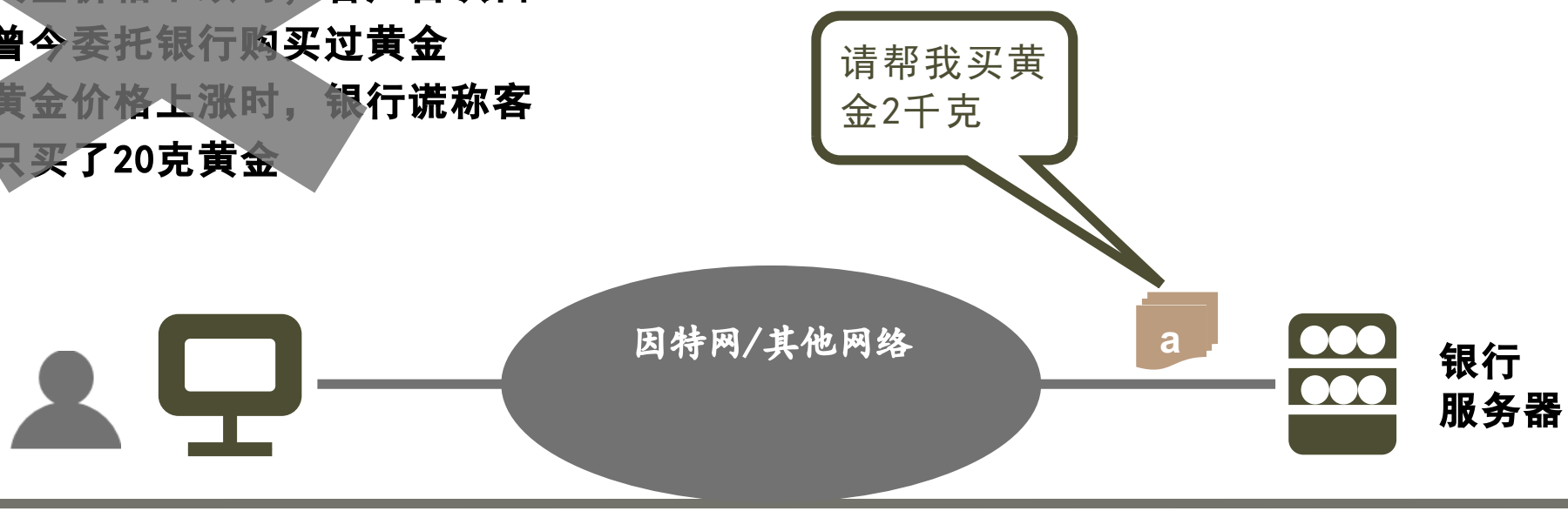
不可否认性/认可性（ Nonrepudiation ）：
发送者不可否认自己发送的信息内容。

不可否认系统特性

- 接收方可以验证发送方所声称身份
- 发送方以后不能否认该消息的内容
- 接收方不可能自己编造这样的消息

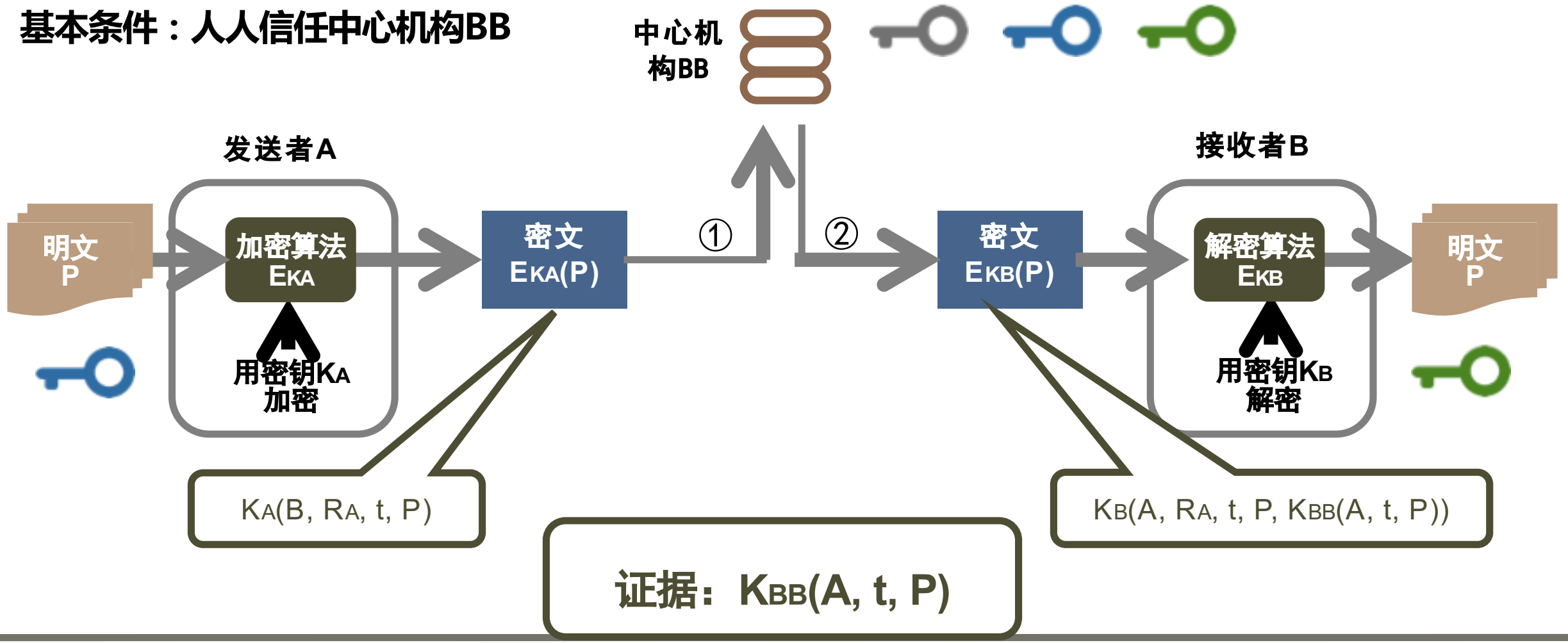
示例：客户和银行有委托买卖关系

- 当黄金价格下跌时，客户否认自己曾令委托银行购买过黄金
- 当黄金价格上涨时，银行谎称客户只买了20克黄金



对称密钥数字签名

基本条件：人人信任中心机构BB



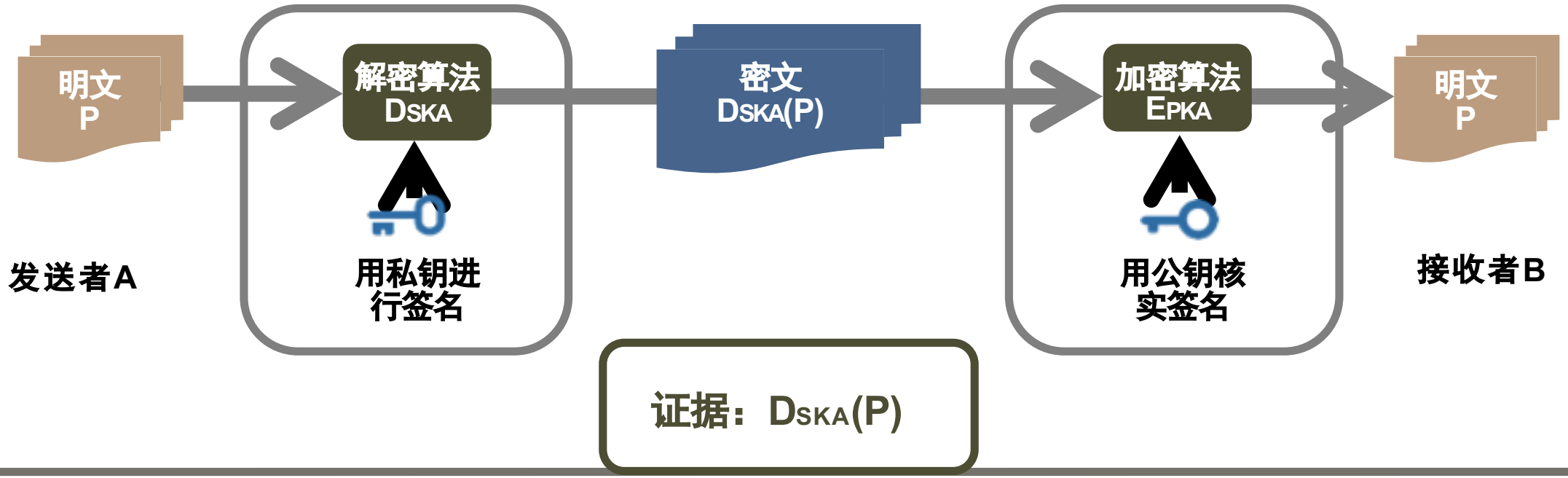
BB的密钥KBB　B的密钥KB　A的密钥KA

公开密钥数字签名

公开密钥算法特性

- D (E(P)) = P
- E (D(P)) = P

- 发送者对于自己的签名用私钥加密
- 接收者用公钥验证发送者的签名



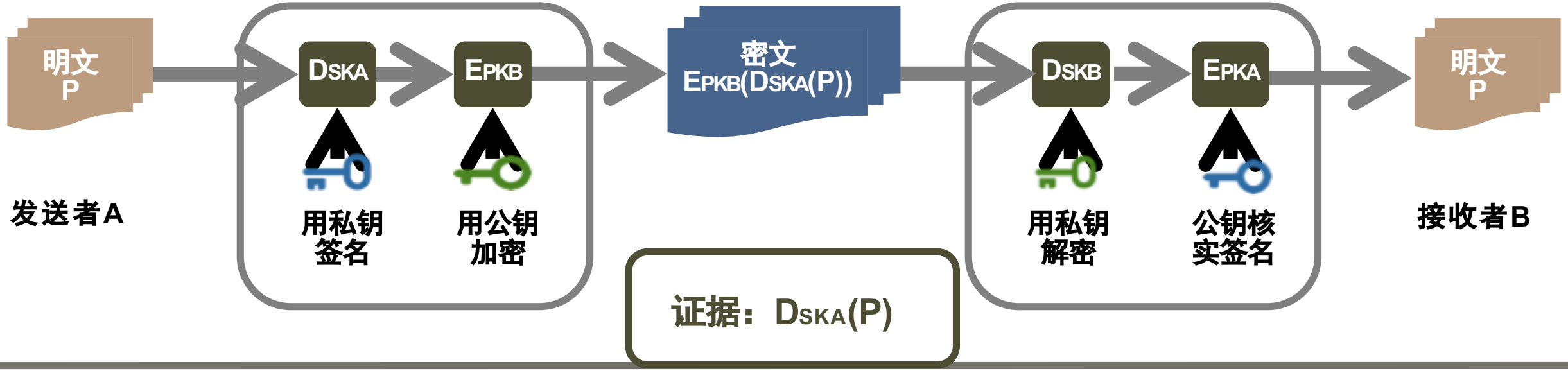
A公钥PKA　A私钥SKA　B公钥PKB　B私钥SKB

带加密功能的公开密钥数字签名

保密性数字签名特点

- 签名并未对发送的信息进行加密
- 公钥可以通过多种途径获得

- 发送者对于自己签名用私钥加密
- 发送者用接收者公钥对消息加密
- 接收者用发送者公钥验证签名
- 接收者用自己私钥对消息解密



A公钥PKA　A私钥SKA　B公钥PKB　B私钥SKB