
RFID安全协议解析

RFID的安全

主要感知层安全，包括RFID安全威胁和安全关键技术。

重点：RFID安全威胁和防护技术

内容：RFID安全主要技术

2、密码相关技术

密码相关技术除了可实现隐私保护，还可以保护RFID系统的机密性、真实性和完整性，并且密码相关技术具有广谱性，在任何标签上均可实施。但完善的密码学机制一般需要较强的计算能力，对标签的功耗和成本是一个较大的挑战。迄今为止，国内外的学者对RFID安全协议进行了大量研究，并设计和提出了大量用于各种场合和环境的安全认证协议。

① 基于Hash函数的安全通信协议

② 基于随机数机制的安全通信协议

③ 基于服务器数据搜索的安全通信协议

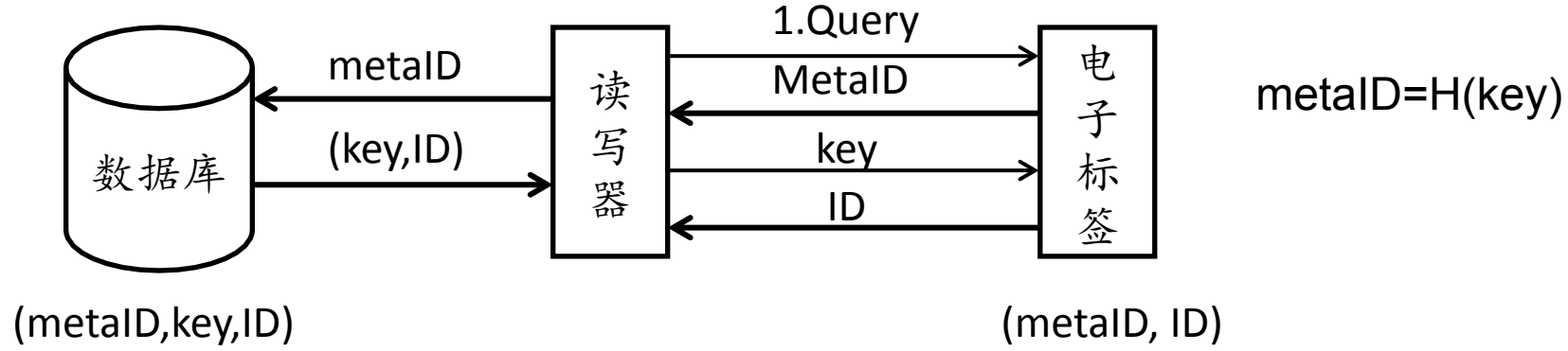
④ 基于逻辑算法的安全通信协议

⑤ 基于重加密机制的安全通信协议

⑥ 基于加密算法的安全认证协议

（1）基于Hash函数的安全通信协议

① Hash锁协议

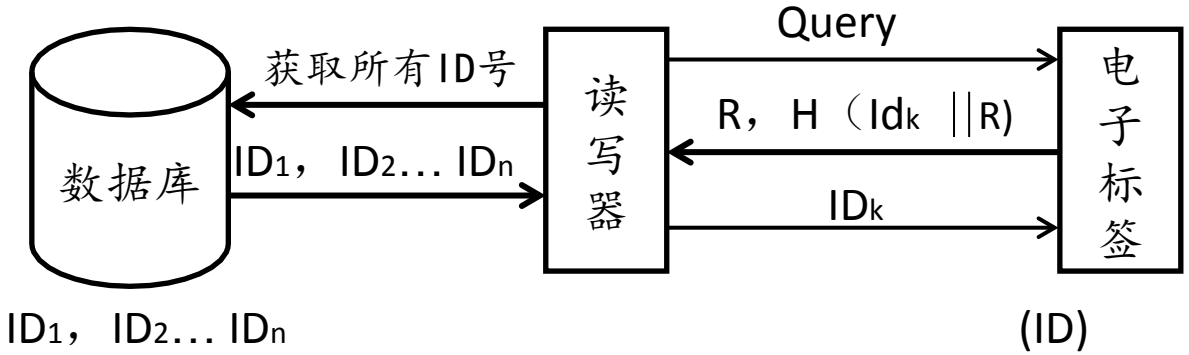


在初始化阶段，每个标签有一个ID值，并指定一个随机的Key，计算metaID=Hash(Key)，把ID和metaID存储在标签中。后端数据存储每一个标签的密钥Key，metaID、ID。

优点：标签运算量小，数据库查询块，实现了标签对读写器的认证；
缺点：空中数据不变，明文传递，标签可被跟踪、窃听和克隆；重放攻击、中间人攻击、拒绝服务攻击均可奏效。

（1）基于Hash函数的安全通信协议

② 随机Hash-Lock协议　采用基于随机数的询问-应答机制。



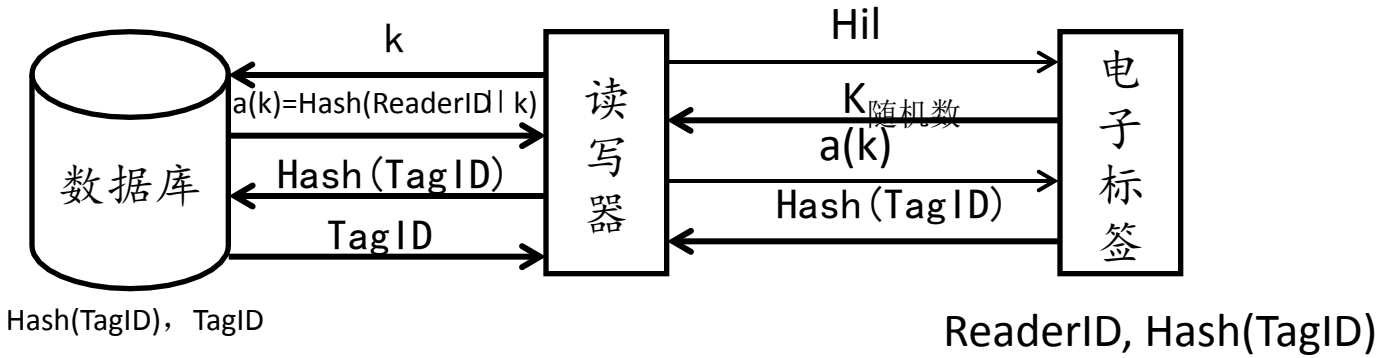
标签除HASH函数外，嵌入了伪随机数发生器，后端数据库存储所有标签的ID。阅读器首先查询标签，标签返回一个随机数R和H（IDK|R),阅读器对数据库中的所有标签计算H（IDK|R)，直到找到相同的HASH为止。

优点：解决了标签隐私性问题；实现了阅读器对标签认证

1、标签计算两次，工作量大；
2、读写器计算所有ID，计算量大；
3、不能防止重放攻击
4、发送ID_k，暴露

（1）基于Hash函数的安全通信协议

③ 供应链RFID协议

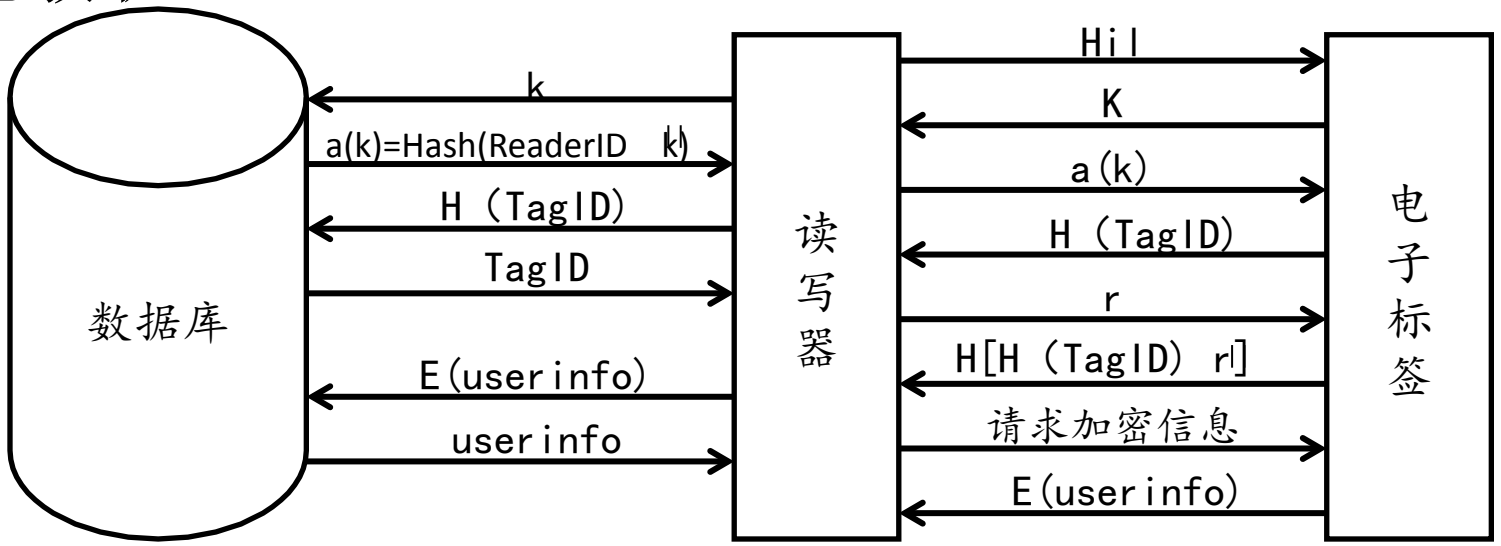


协议解决了机密性、真实性和隐私性问题。简单明了，数据库查询速度快。

1、标签需要Hash，增加了标签成本、功耗和运行时间；
2、不能防止重放攻击；
3、监听Hash（TagID），跟踪标签；
4、阅读器管理TID，难度大
5、一个地点的所有标签共享同一个ReaderID,安全性不高。

（1）基于Hash函数的安全通信协议

④ 相互认证RFID安全系统（改进上个协议：标签认证和加密信息获取）



Hash(TagID)，TagID

E(userinfo)，userinfo

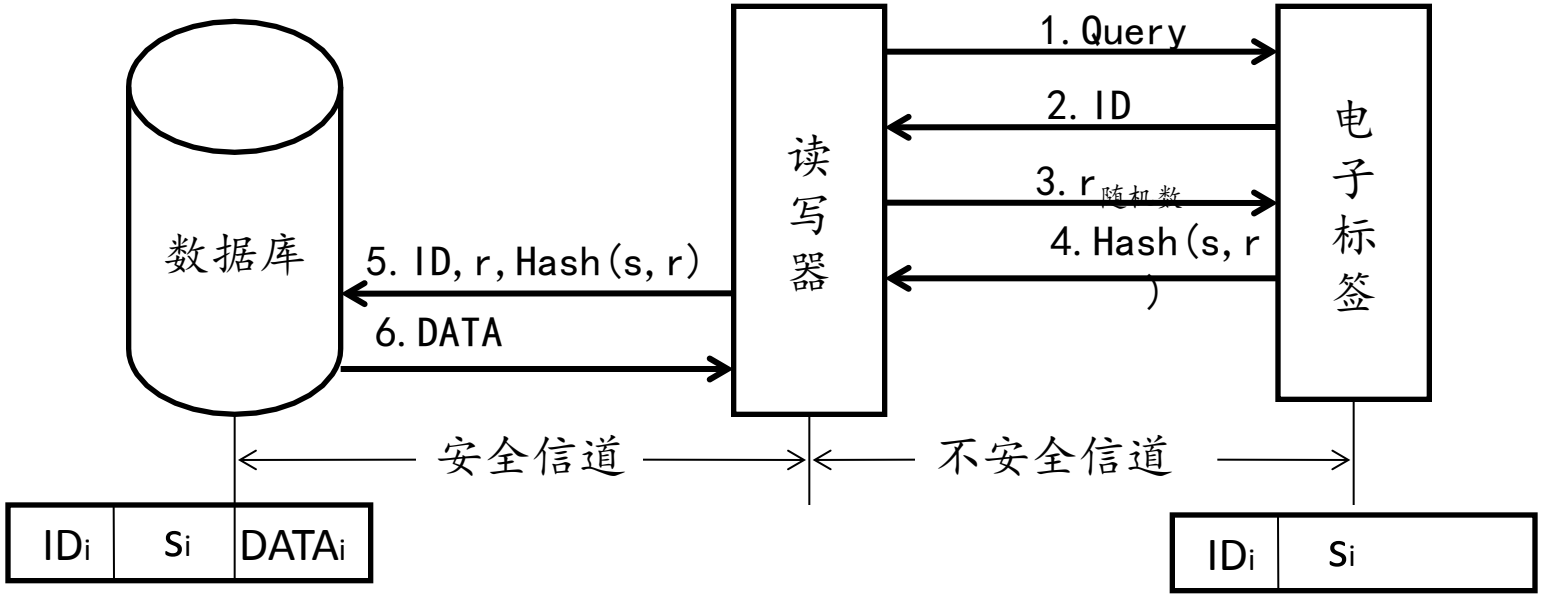
ReadID, Hash(TagID)

E(userinfo)

1标签需要Hash；2、不能防止重放攻击；3、E(userinfo)加重跟踪标签；4、阅读器管理TID，难度大，管理userinfo，多事

（1）基于Hash函数的安全通信协议

⑤ 移动型RFID安全协议

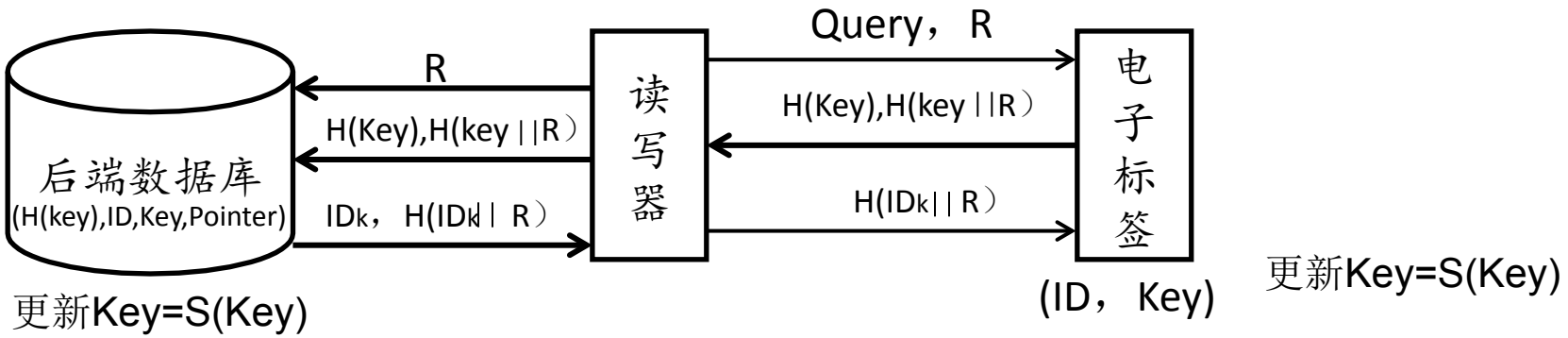


协议解决了机密性、真实性和隐私性问题。简单明了。

1标签需要Hash；2、不能防止重放攻击；3、ID不变，跟踪标签；4、管理秘密值S_i难度大因为系统越大，S_i越多。

（1）基于Hash函数的安全通信协议

⑥ Reader-Tag安全协议流程

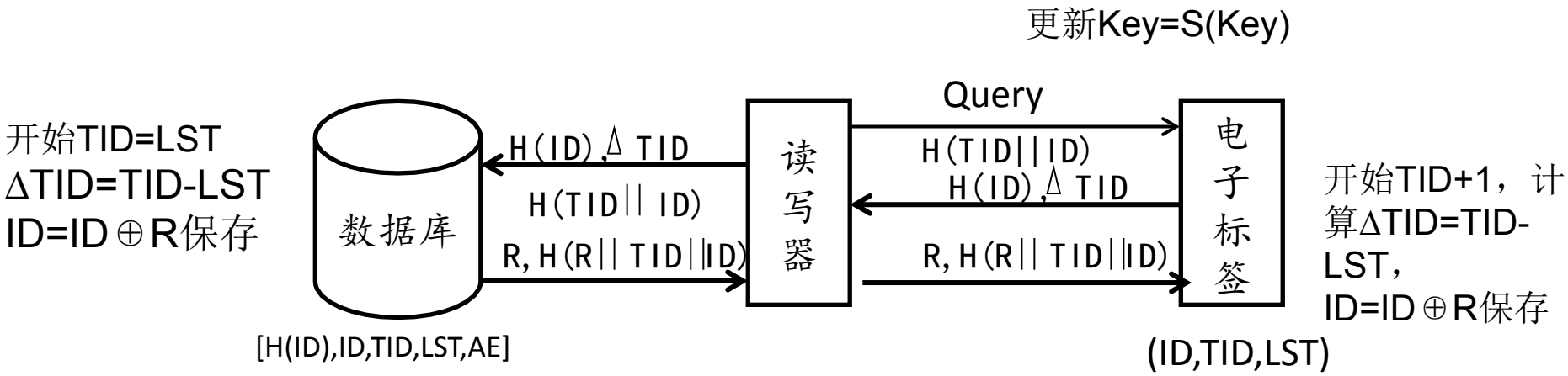


协议解决了机密性、真实性和隐私性问题。数据库搜索速度快，并可从失步中恢复。

1、标签需要2个Hash，4次计算；
2、攻击者可以发同一R，跟踪标签；
3、标签存在数据更新问题，识别距离减半。

（1）基于Hash函数的安全通信协议

⑦ 基于Hash的ID变化协议

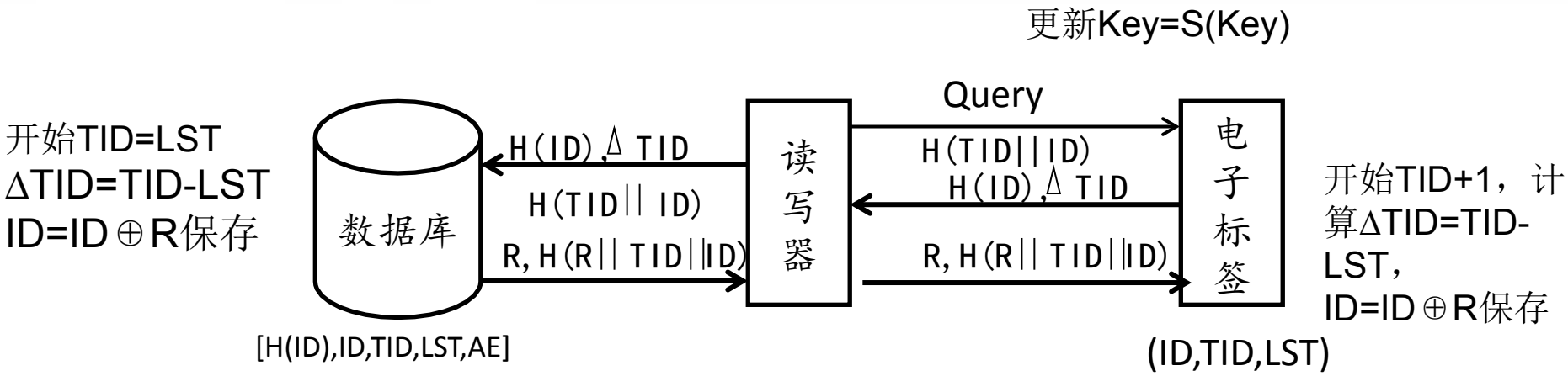


初始状态：标签存储ID，TID（上次发送序号，LST（最后发送序号），且TID=LST；后端数据库存储（HID）、ID、TID、LST、AE）。

在每一次认证过程中都改变了与阅读器交换的信息。每次会话TID都会加1,TID加1导致Hash值每次不一样，避免跟踪，比较复杂

（1）基于Hash函数的安全通信协议

⑦ 基于Hash的ID变化协议



1、阅读器向标签发送查询命令；

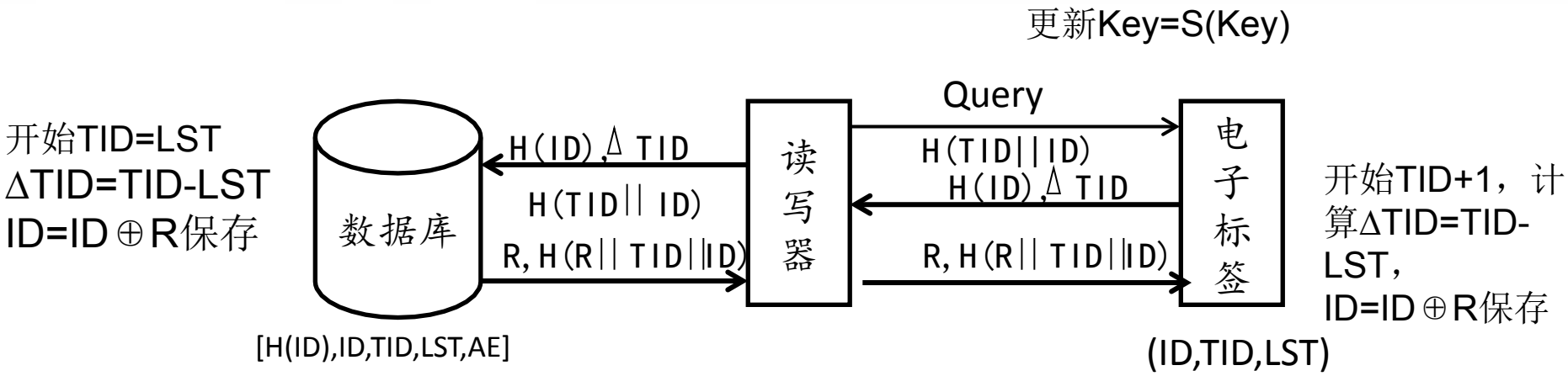
2、标签将自身TID加1，计算H（ID），ΔTID=TID-LST，H（TID||ID），然后将3个值发送给阅读器；阅读器将收到的3个数转发给数据库；

3、数据库根据H（ID），搜索标签，找到后利用TID=LST+ ΔTID计算出TID，然后计算H（TID||ID），并与接收到的标签数据比较，如果相等则通过认证；通过认证后，更新TID、LST=TID及ID=ID ⊕R，其中R是随机数，然后数据库计算H（R||TID||ID），并随R一起发送给阅读器；阅读器转发给标签；

4、标签利用自身保存的TID、ID及收到的R计算H（R||TID||ID），判断是否与收到的是否相等，相等则通过认证，更新LST=TID， ID=ID ⊕R

（1）基于Hash函数的安全通信协议

⑦ 基于Hash的ID变化协议



特点：TID加1导致Hash值每次都不同，避免跟踪。

问题：

1、干扰造成不同步；

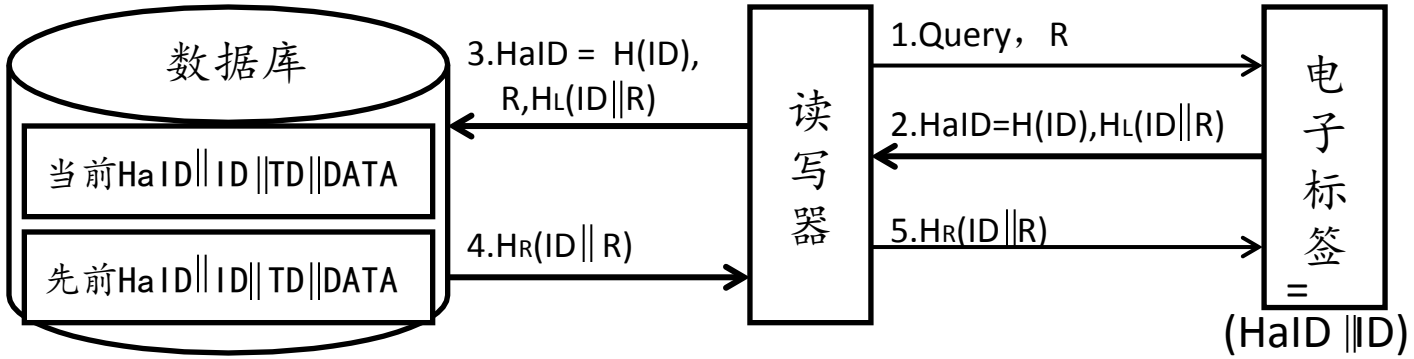
2、攻击者发送查询命令，记录第二步的三个记录，发给阅读器，从而使数据库更新，造成不同步；

3、攻击阻止阅读器发给标签，也可造成不同步；

4、攻击者发送两次查询，可以跟踪标签

（1）基于Hash函数的安全通信协议

⑧ LCAP协议（连接控制访问协议）



LCAP协议的执行过程如下：

（1）读写器生成一秘密随机数R，向标签发送Query认证请求，将R发送给标签；

（2）标签计算HaID=H（ID）和H_L（ID||R），其中ID为标签的标识，H_L表示Hash函数H输出的左半部分，标签将（HaID，H_L（ID||R））发送给读写器；

（3）读写器将（HaID，R，H_L（ID||R））发送给后台数据库：

（1）基于Hash函数的安全通信协议

（4）后台数据库查询预先计算好的Hash值Hash（ID）是否与所接收到的HaID一致。如果一致，认证通过，更新数据库中的ID= ID⊕R，相应更新Hash值，以备下次查询；然后用旧的ID计算H_R（ID||R），并通过阅读器转发给标签；

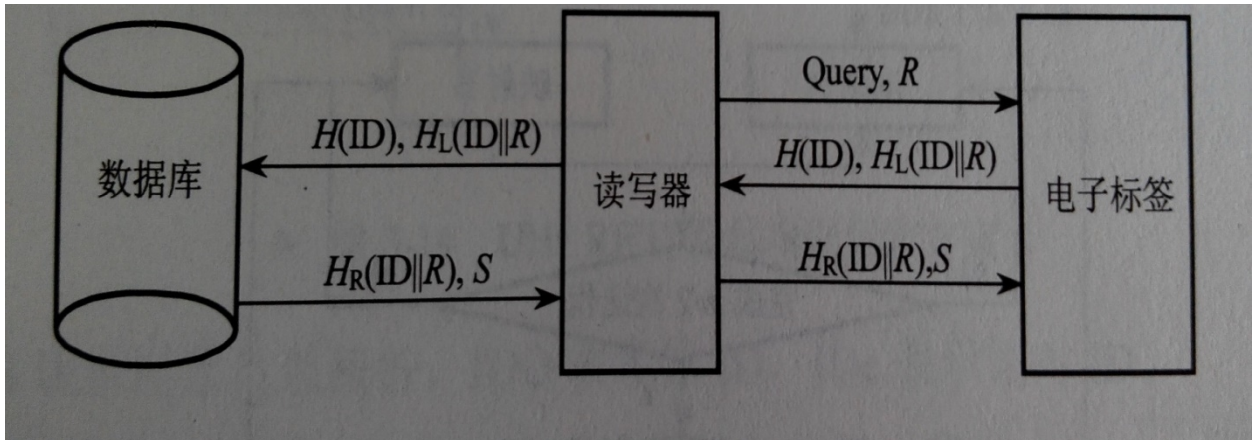
（5）标签验证H_R（ID||R）的有效性，如果有效，则更新其ID为ID=ID⊕R。

协议解决了机密性、真实性和隐私性问题。并且数据库可预先计算H(ID)，数据库搜索速度快。

缺点：1、标签需要Hash；2、两次请求可以获得H(ID)，跟踪标签；3、攻击造成不同步；4、ID有可能与其他标签一致；标签不能抵抗重放攻击，因为用同样的R(可以截获)和H_R（ID||R），这样可以重放了；5、攻击和干扰可造成ID不同步。

（1）基于Hash函数的安全通信协议

⑨ LCAP改进协议



区别更新ID=ID⊕S，非ID=ID⊕R，S由数据库选择，这样保证ID的唯一性，但S明文传送，容易篡改，如果S全0，ID异或没有变化，容易跟踪，且造成数据库与标签不同步。

（1）基于Hash函数的安全通信协议

⑩RFID反跟踪安全通信协议

标签和数据库共享密钥K，K同时作为标签的标志。标签存储一个可更新的时间戳Tt，并实现一个带密钥的Hash函数Hk。数据库保存一个时间戳Tr。Tr每隔一定周期变化一次，当其变化时数据库预先计算并保存所有标签的Hash值Hk（Tr）。

1、读写器发送当前时间戳Tr到标签；

2、标签比较时间戳Tr与Tt，若Tr大于Tt，则阅读器合法，用Tr更新Tt，计算并返回Hk（Tr）；

3、后端数据库搜索标签返回值，若有效则认证通过。此处Tr作为时间戳。

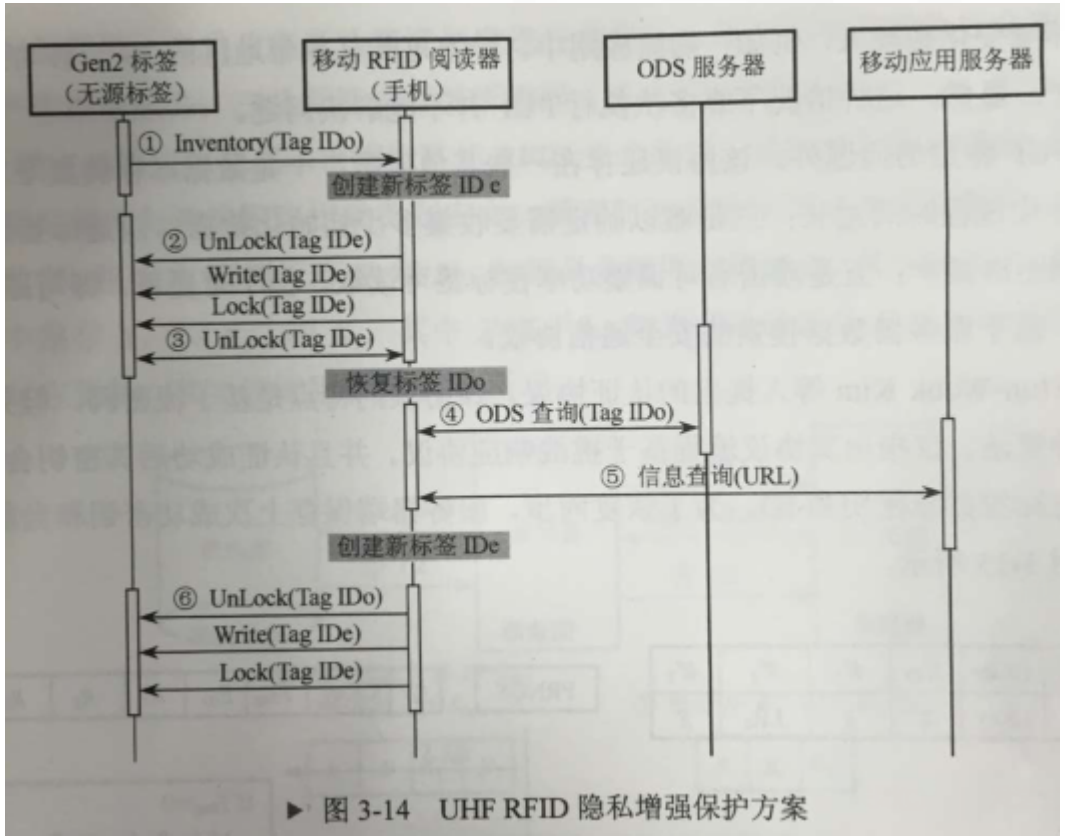
协议解决了机密性、真实性和隐私性问题。提出了通过时间戳的自然变化防止标签跟踪，数据库也预先计算，搜索速度快。并且数据库可预先计算H(ID)，数据库搜索速度快。

缺点：Tr不具有机密性，伪造Tr通过认证；计算量大，识别距离减半

（2）基于随机数机制的安全通信协议

①UHF RFID隐私增强保护方案（移动电话）

设想：用户购买商品后马上把标签的原ID结合随机数加密后生成新的ID写入标签。当需要根据ID查询商品信息时，再用手机解密，并且再次生成并写入新的随机密文。



▶ 图 3-14　UHF RFID 隐私增强保护方案

优点：简单，标签不需要增加任何功能。
缺点：用户手机需要集成阅读器；
用户需要不时对标签加密，商品数量多时困难l；
密钥管理困难；
未考虑相互认证。

（2）基于随机数机制的安全通信协议

②基于PUF的安全和隐私方案

PUF(Physical Unclonable Functions)是一组微型延迟电 路，利用提取芯片制造过程中不可避免产生的差异，生成无限多个、唯一的、不可预测的“密钥”。这些密钥是动态 随机生成的，它使用口令/响应机制进行验证。PUF 系统收到 一个随机的 64 位的代码后，会同时生成一个唯一的随机的 64 位(或者更长)代码作为响应。由于芯片制造过程中产生的 差异本身具有不可模仿和复制的特性，即使是芯片的制造厂 商也不可能从另外一个芯片上复制出一套一模一样的口令响 应序列。因此，PUF 技术使得芯片具有反仿制的功能。PUF 判优电路的工作原理如图 1 所示。

在低成本 RFID 系统中使用 PUF 电路有一些 好处：

- 对于同样的输入，2 个 PUF 不大可能产生同样的输出。因此PUF具有很好的抗物理攻击性能
- 输出结果不能通过数学运算产生，因此，它不能被 预测。
- 64 位 PUF 实现只需要 545 门。