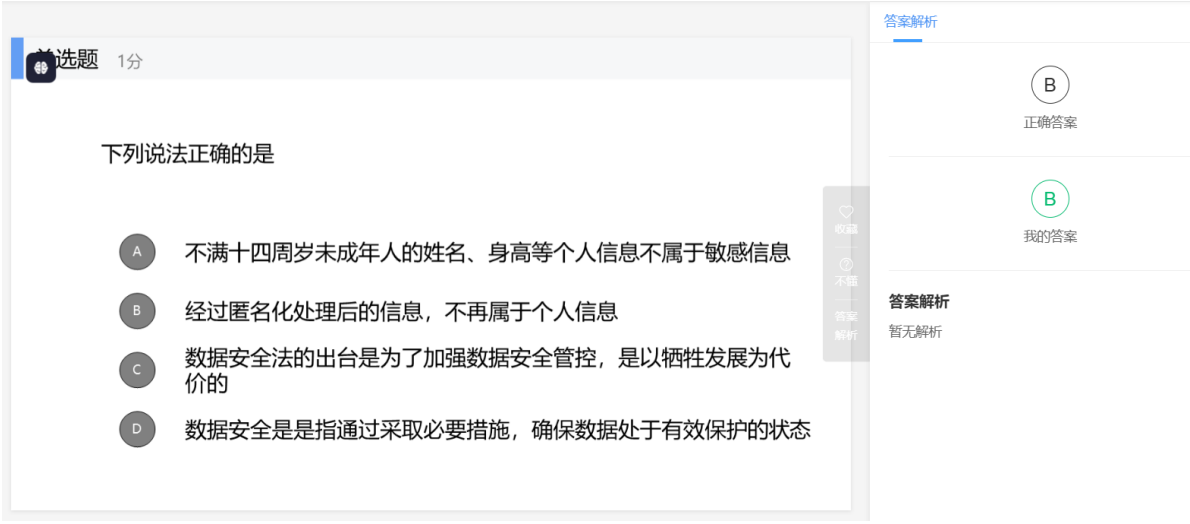
数据安全雨课堂答案

2024 Spring

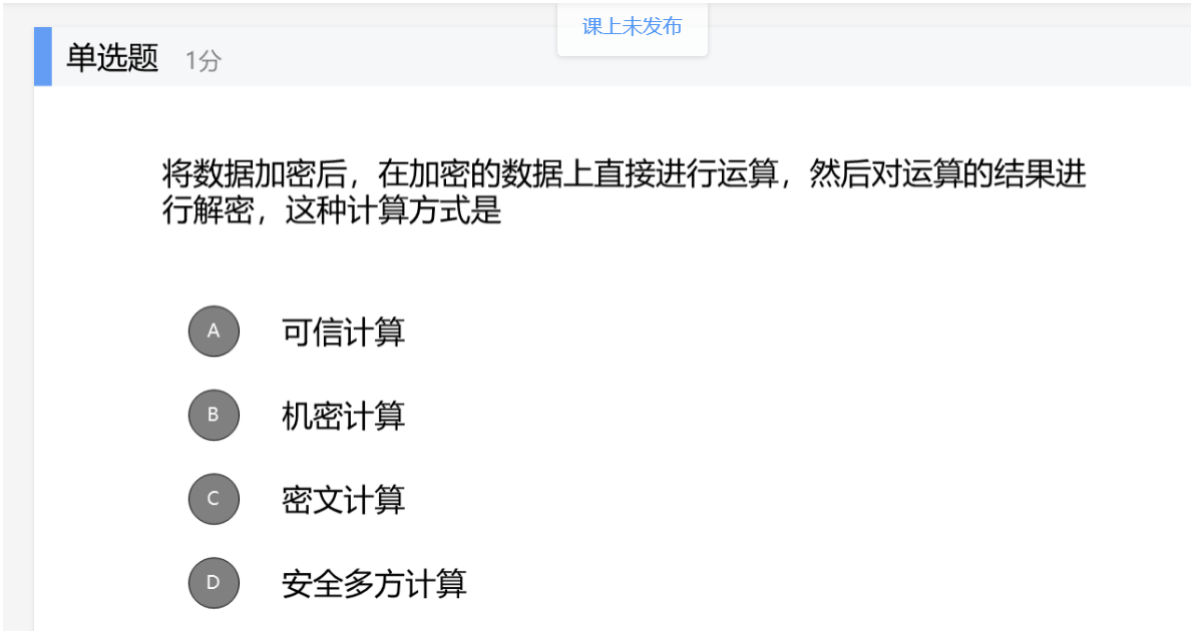
2025.2.21 by Erwin Zhou

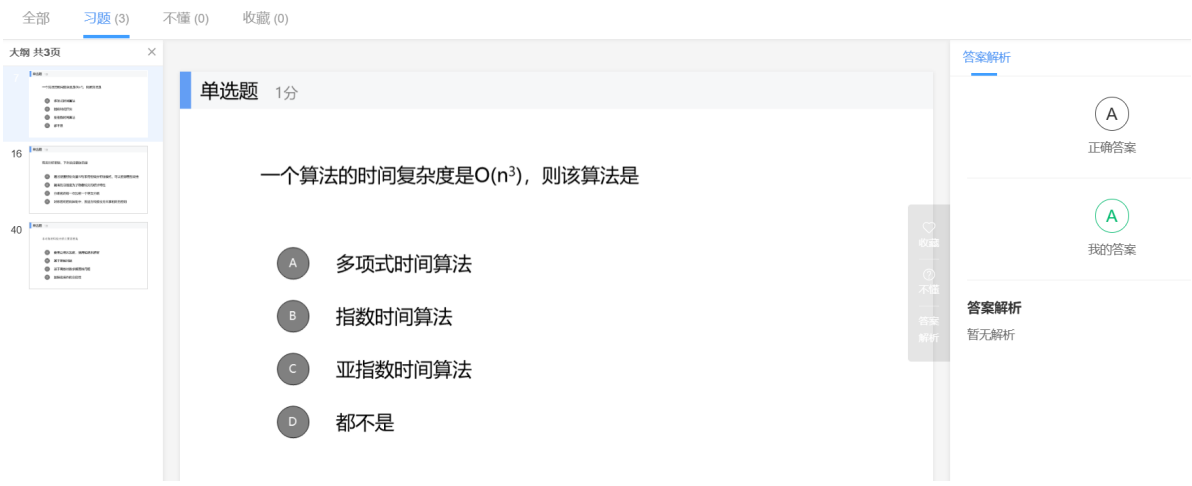
00



01

)


课上未发布
单选题 1分
将数据加密后，在加密的数据上直接进行运算，然后对运算的结果进行解密，这种计算方式是
A 可信计算
B 机密计算
C 密文计算
D 安全多方计算

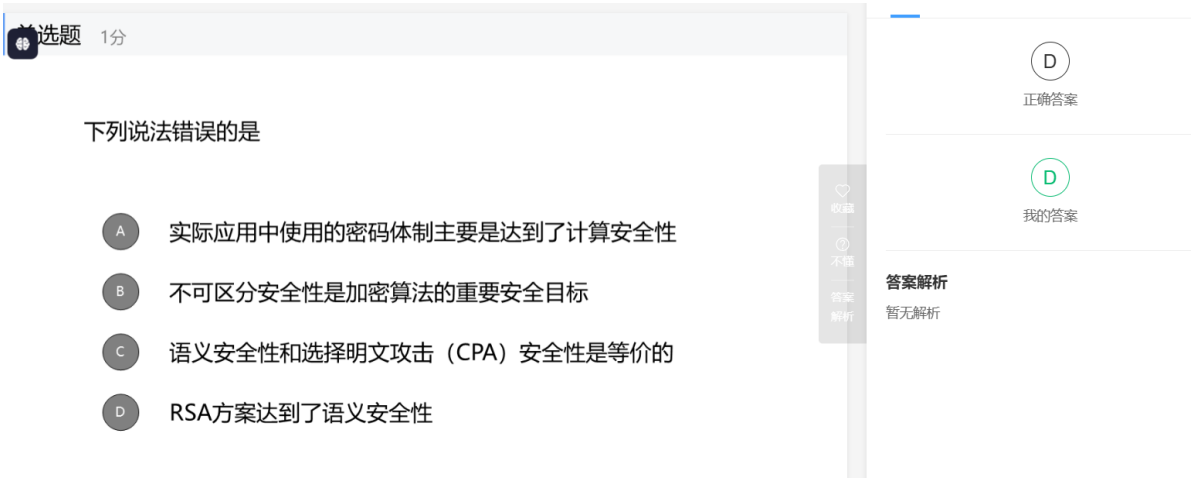

全部
习题 (3)
不懂 (0)
收藏 (0)
大纲 共3页
单选题 1分
一个算法的时间复杂度是O(n³)，则该算法是
A 多项式时间算法
B 指数时间算法
C 亚指数时间算法
D 都不是
答案解析
A
正确答案
A
我的答案
答案解析
暂无解析


关闭
全部
习题 (3)
不懂 (0)
收藏 (0)
打印课件
大纲 共3页
选题 1分
有关对称密码，下列说法错误的是
A 通过设置初始向量IV和采用密码分组链模式，可以抵御重放攻击
B 混淆的目的是为了隐藏明文的统计特性
C 分组密码每一次加密一个明文分组
D 对称密钥密码体制中，发送方和接收方共享相同的密钥
答案解析
B
正确答案
B
我的答案
答案解析
暂无解析


课上未发布
单选题 1分
非对称密码设计的主要思想是
A 使用公钥来加密，使用私钥来解密
B 基于难解问题
C 基于离散对数求解困难问题
D 加解密操作的交换性

03


单选题 1分
有关密码学中的安全性，说法错误的是
A 如果对密码系统的某类攻击是可忽略事件，那么在设计密码时，就无需考虑这种攻击
B 通过已知的明文-密文对，推测出其他一些密文对应的明文信息的攻击是已知明文攻击
C 计算安全性是信息论安全性
D 一次一密是达到完美安全的设计方法，它要求每次均使用随机变化的密钥进行加解密
答案解析
C
正确答案
C
我的答案
答案解析
暂无解析


单选题 1分
下列说法错误的是
A 实际应用中使用的密码体制主要是达到了计算安全性
B 不可区分安全性是加密算法的重要安全目标
C 语义安全性和选择明文攻击（CPA）安全性是等价的
D RSA方案达到了语义安全性
D
正确答案
D
我的答案
答案解析
暂无解析

04

单选题 1分

有关同态加密说法错误的是

A 计算方可以在同态加密算法输出的密文上做计算

B 同态加密求值函数输出的密文可以被解密

C 同态加密的语义安全性意味着相同的明文应该加密成不同的密文

D 类同态加密能同时支持多种同态操作(加或乘同态)，并可以在安全参数中定义能够执行的操作次数上限

收藏 不错 答案解析

答案解析

正确答案 D

我的答案 D

答案解析

暂无解析

课上未发布

单选题 1分

能够同时支持多种同态操作(加或乘同态)，并可以在安全参数中定义能够执行的操作次数上限的同态加密是

A 半同态加密

B 类同态加密

C 层级同态加密

D 全同态加密

我的选项：C 正确答案：C

单选题 1分

下列哪个同态加密方案可以支持浮点数运算

A Paillier

B Gentry

C CKKS

D GSW

我的选项：C　　正确答案：C

单选题　1分

有关Paillier算法，说法错误的是

A　Paillier依赖的数学难题是判定复合剩余假设

B　Paillier可以用在密文上的求和平均值等运算

C　Paillier支持标量乘法，也就是密文与密文的乘积运算

D　Paillier属于半同态加密算法

05

单选题　1分

整数模5加法群Z_5={0，1，2，3，4}，其群的阶为5，单位元为0。元素2的阶为

A　2

B　3

C　4

D　5

收藏　不懂　答案解析

答案解析

D
正确答案

D
我的答案

答案解析

暂无解析

单选题　1分

有关方案BGN，说法错误的是

A　属于类同态加密

B　支持任意多次乘法，但仅支持一次加法

C　所采用的双线性映射为可采纳的双线性映射

D　循环群比较容易构造加法同态

收藏　不懂　答案解析

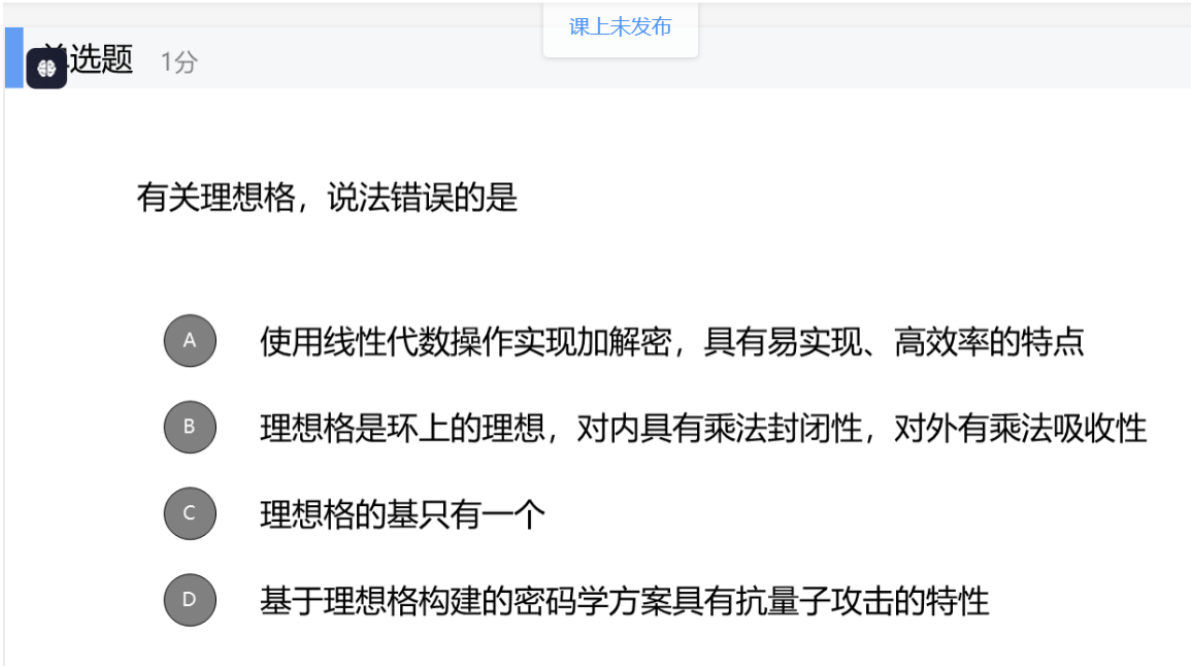
答案解析

B
正确答案

B
我的答案

答案解析

暂无解析


课上未发布
选题 1分
有关理想格，说法错误的是
A 使用线性代数操作实现加解密，具有易实现、高效率的特点
B 理想格是环上的理想，对内具有乘法封闭性，对外有乘法吸收性
C 理想格的基只有一个
D 基于理想格构建的密码学方案具有抗量子攻击的特性

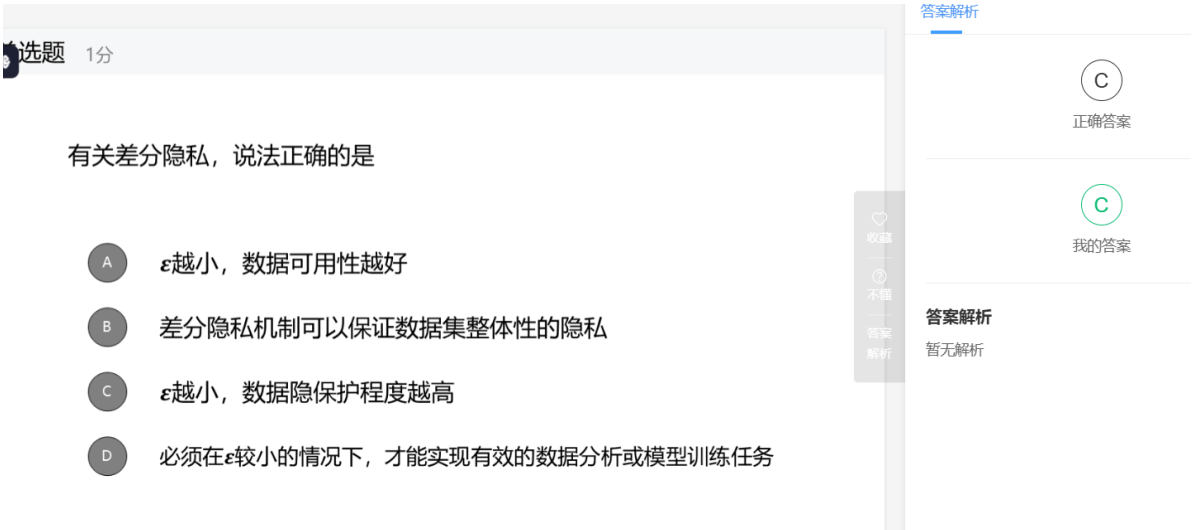
06

无

07


单选题 1分
有关Shamir秘密共享，说法错误的是
A 可以基于解方程法来实现秘密重构
B 可以基于多项式插值法来实现秘密重构
C 具有不受限制的加法同态性质
D 具有无限的乘法同态性质
答案解析
D
正确答案
D
我的答案
答案解析
暂无解析

09


选题 1分
有关差分隐私，说法正确的是
A ε越小，数据可用性越好
B 差分隐私机制可以保证数据集整体性的隐私
C ε越小，数据隐保护程度越高
D 必须在ε较小的情况下，才能实现有效的数据分析或模型训练任务
答案解析
C
正确答案
C
我的答案
答案解析
暂无解析

课上未发布

单选题 1分

有关差分隐私，说法错误的是

A 非交互式数据发布，后续查询不会消耗隐私预算

B 差分隐私的并行组合特性，是指数据集中每条记录的隐私损失将不超过全部所有算法导致的隐私损失的总和

C 与数据集无关的映射f与一个满足(ε, δ) −差分隐私的算法M组合起来，仍然满足(ε, δ) −差分隐私

我的选项：C 正确答案：C

单选题 1分

在交互式发布中，假定隐私预算为ε，允许的查询次数为k，则每次查询分配的预算为

A ε

B k

C ε/k

D εk

我的选项：A 正确答案：A

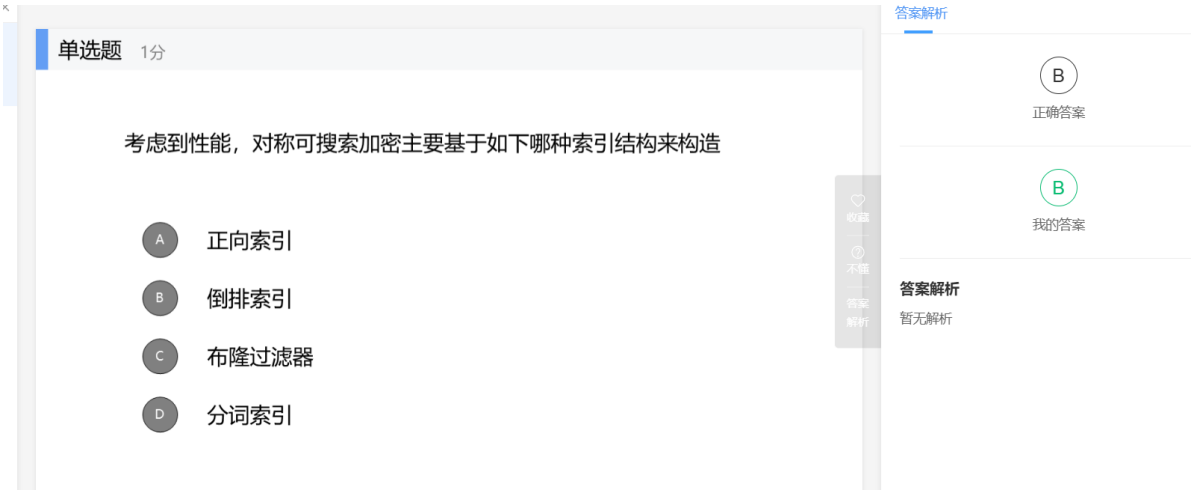
单选题 1分

随机响应机制中，校正的作用是

A 解决扰动性带来的噪音问题，实现结果的纠偏

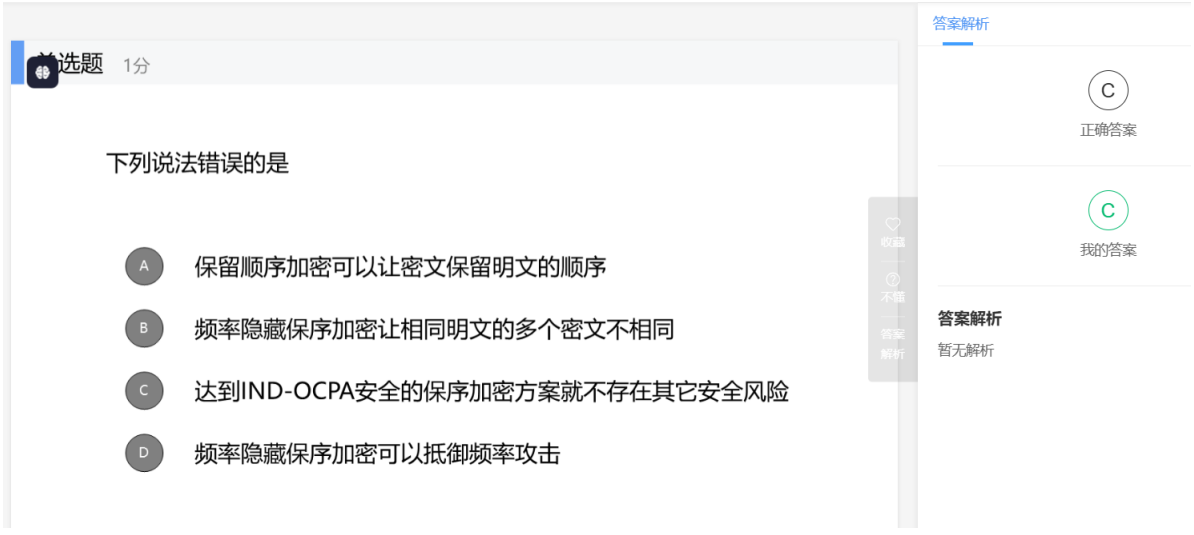
B 添加噪音，达到差分隐私的效果

10


单选题 1分
考虑到性能，对称可搜索加密主要基于如下哪种索引结构来构造
A 正向索引
B 倒排索引
C 布隆过滤器
D 分词索引
收藏
不懂
答案解析
答案解析
B
正确答案
B
我的答案
答案解析
暂无解析


单选题 1分
文件注入攻击利用了可搜索加密的哪种模式泄露?
A 查询模式
B 大小模式
C 访问行为模式
D 以上都不是
收藏
不懂
答案解析
答案解析
A
正确答案
A
我的答案
答案解析
暂无解析

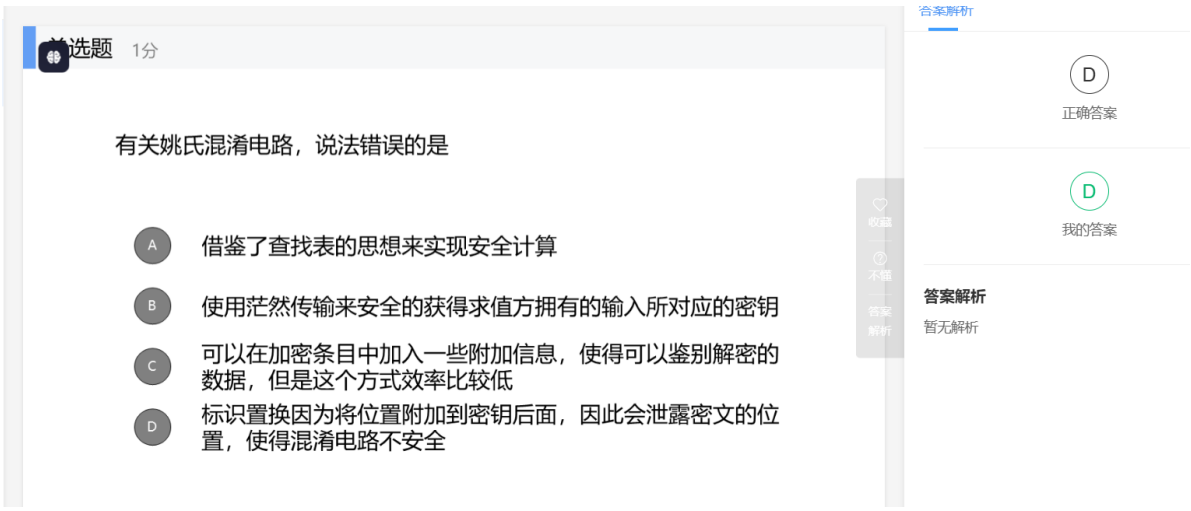
11


单选题 1分
下列说法错误的是
A 保留顺序加密可以让密文保留明文的顺序
B 频率隐藏保序加密让相同明文的多个密文不相同
C 达到IND-OCPA安全的保序加密方案就不存在其它安全风险
D 频率隐藏保序加密可以抵御频率攻击
收藏
不懂
答案解析
答案解析
C
正确答案
C
我的答案
答案解析
暂无解析

12

无

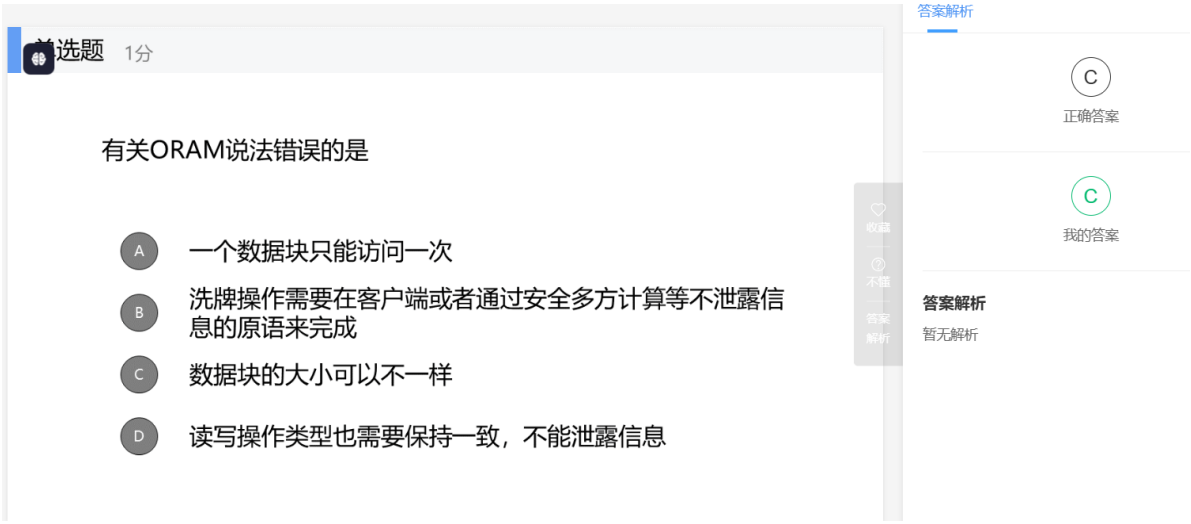
13



14

无

密码应用与访问行为模式保护



选题 1分

有关多云ORAM的洋葱加密说法错误的是

A 洋葱加密就是多次加密，每次采用不同的密钥

B 多云ORAM的洋葱加密是避免相同的块被识别出来

C 对于多云ORAM而言，洋葱加密能保证安全，不再需要洗牌操作

D 多云ORAM的多次读写加密会造成洋葱加密层的层数不一致

收藏 不错 答案解析

答案解析

C
正确答案

C
我的答案

答案解析

暂无解析