上海交通大学在线考试诚信承诺书

SJTU Online Examination Honor Code Letter

考试不仅是对学习成效的检查，更是对道德品质的检验。自觉维护学校的考风考纪，营造公平、公正的考试环境是全体同学的共同责任和义务。特别在疫情防控的特殊时期，更应强化自律意识，恪守诚信，拒绝舞弊，做一名诚实守信的新时代大学生，用诚信的考试构筑诚信的人生。

Examination is the evaluation of both learning effect and morality. It is the responsibility and obligation of all students to consciously maintain the school's common examination practice, abide by the discipline and create a fair and just examination environment. Especially in the special period of epidemic prevention and control, we should strengthen the consciousness of self-discipline, abide by the integrity, refuse to cheat, be an honest and trustworthy college student in the new era, and build an honest life from the integrity test.

我郑重承诺 I solemnly promise：

（1）本人将履约践诺，知行统一；遵从诚信规范，恪守学术道德；自尊自爱，自省自律。I will fulfill my promise, unify between knowledge and action, abide by the rules of integrity, academic ethics, be self-respected and self-disciplined.

（2）在线考试过程中，自觉遵守学校和老师宣布的考试纪律（详见《上海交通大学本科生学生手册》中的《学生考试纪律规定》，沪交教【2019】28 号），不剽窃，不违纪，不作弊。In the process of online examination, I will consciously abide by the examination discipline announced by the school and the teachers (see the regulations on student examination discipline in the undergraduate student handbook of Shanghai Jiao Tong University, HJJ [2019] No. 28), and do not plagiarize, violate discipline or cheat.

（3）若违反相关考试规定和纪律要求，自愿接受学校的严肃处理或处分。In case of violation of relevant examination regulations and discipline, students shall bear the serious treatment or punishment from the school.

承诺人 Committed by：李昱翰

（学号 Student No：5220021910279）

日期 Date (Y/M/D)：2023年1月5日

上 海 交 通 大 学 答 题 纸

（ 2022至 2023学年 第 1 学期 ）

班级号 F2003702　　学号 5200219202779　　姓名 李昱翰

课程名称 计算机系统工程　　成绩 _____

我承诺，我将严格遵守考试纪律。

承诺人：李昱翰

题号										
得分										
批阅人(流水阅卷教师签名处)										

oblem 1: Transaction:

a. time 2: A10　　time 2: B15

b. abort: T1, T2　　commit: T2, T3, T4

c. A: A27　　B: B25

d. ①: 不是 serializable 的。②: 因为对于 T3, T4 若先执行 T3, 那么 T4 不应当在 R(B) 读到 B15, 若 T4 比 T3 先执行, T3 在 R(A) 也不应读到 A10, 所以不是 serializable 的.

e. ①: single machine: 可以使用一个 global counter, 并用 Fetch And Add 进行 "+1" 操作。

②: distributed machine: 每个 machine 使用本地时钟, 并定时与一些 time server 同步, 可使用类似 spanner 的 TrueTime 进行同步

上海交通大学答题纸

（ 2022至2023 学年 第 1 学期 ）

课程名称 计算机系统工程

姓名 李昊翰 学号 5220219079

2. a. ①不能。②：因为在t1时已经过了 prepare 阶段，故 worker2 需要等待 coordinator restart 重新发送 commit/abort request 才可以进一步操作。

b. ①：由于 worker1 reply not ok，所以 coordinator 会使整个 transaction abort

②：若 worker2 在 t1 之前恢复，在其 restart 之后会 redo logs，发送 ~~重新向 coordinator~~ 并会接受到 coordinator 的 request 并将自己的 sub-transaction abort.

③：若 worker2 在 t1 之后恢复，在其 restart 之后，通过 redo/undo log 发现自己 t1 前的 sub-transaction 已经 abort，故直接 undo 对应事务的 log。

c. ①：~~2PC 在 prepare 阶段若 coordinator crash，~~
2PC 中，只有 coordinator 能发出 requests，worker 接收到 requests 并正确地响应 requests 系统才能 commit/abort，所以 machine crash 时可能需要大量 retry，使可用性下降，并且在 commit 前 crash 只可 abort，故 availability 也较差

② possible solution：~~对于只读事务可只使用 MVCC 进行控制~~
使用 RSM，paxos 等来实现 replicated consistency，并保证高可用性。

上 海 交 通 大 学 答 题 纸

（ 20 22 至 20 23 学年 第 1 学期 ）

课程名称 CSE 姓名 翟翰 5720021910279

Problem 2: Network:

1. C's advertisement: [(B, 3), (A, 8), (D, 5)]

E's advertisement: [(A, 6), (D, 3)]

A's routing table:

dst	route	cost
B	A-B	7.
C	A-D	7.
D	A-D	2
E	A-D.	5.

a. N5 → N70 → N79 → N90 (have key 89).

b. ①: 不会成功发送

②每个节点不光要有你自己的 finger table，并且还要有你一些后继节点相对的链表，并在后继节点 crash 时更新这些链表。

3) a. ①: 可纠错1位。②: P1, P2 同时错，P4对，说明P3错；P1, P4 同时错，P2对，说明P5错；P2, P4 错，P1对，说明P6错；若 P1, P2, P4 都错说明 P3 错。

b. ①收到 0110001，有：P1'=0, P2'=0, P4'=1，而 P1=0, P2=1, P4=0，故 P1, P4 与计算结果不同，而 P2=(P3+P6+P7) 为2，P4=(P5+P6+P7) 为2，可正确得 P1=(P3+P5+P7) 为2，故 P3, P5, P7 不能同时错，P5, P7, P3 也不能单独错（不可能同时错两个），故只能是 P6 发生错误。

②: P6 出错。

上海交通大学答题纸

（ 2022 至 2023 学年 第 1 学期 ）

5720021910779

课程名称 CSE 姓名 李昱翰

Problem3: Replication: send <decide, Va> to all nodes.

1. (a): leader 将 Na 设为 Nn+1 将 Va 设为 V, 并开始下一轮 propose

(b): 当 leader 收到有 ~~所有 nodes~~ 发送 <accept, Nn+1, V> delay + restart paxos.
nodes

(c): reject proposal N. (reply <accept-reject>).

(d): Nh = N; Va = V; Na = N;

2. ①: 不正确。

②: example: 若 acceptor 在接受到 accept 请求之后 crash, 那么这个 acceptor 的 Na 就不应该是 Nh 出现了不一致。
而此轮 accept 由于没有 majority 而失败

3. a. ①: S1, S2, S3 可能成为 leader.

②: 因为 S1 若想成为 leader, 只需得到 S1, S3, S5 的 vote 即可, S2 由于有最新的 term3 log, 故其只需获取 S1, S2, S3, S5 中至少3个 vote 即可, S5 与 S1 类似, 只需得到 S1, S3, S5 的 vote 即可。

b. ①: 可以 commit 的 entries:
index 为1 的 term1 log; index 为2 的 term1 log;

②: 其余不可提交原因:

1. 对于 index 为3 的 term1 log, 无 majority;
2. 对于 index 为3 的 term2 log, 虽然其已 majority, 但若 S2 成为 term3 leader 会被 rewrite;
3. 对于 index 为4 的 term2 log, 虽然已为 majority, 但若 S2 成为 term5 leader 会被 rewrite;
4. 对于 index 为4, term3 log, index 为5, term2 log 以及 index 为6 的 term4 log, 由于未达到 majority 而不会被 commit.

上 海 交 通 大 学 答 题 纸

（ 2022至 2023学年 第 1 学期 ）

课程名称 CS6 姓名 李昱翰 5720021910279

不 ①: CAP theorem: 指的是在一个分布式系统，最多可以同时保证 consistency (C), availability (A), network partition (P) 中的两个。

②: Raft 牺牲性能了 availability.

③: 因为 Raft 中每有一个新的 term 都要选个新的 leader，而选取 leader 失败则会导致进入新的 term 并重新选举. 并且每当新的 leader 产生后，其会同步所有 node 的 log entries，这也会使得系统性能较差。

oblem 4: Security:

在 getline 函数中，若 ' 遇到 c=='\n' 会提前返回，这可能使得攻击者通过 计时攻击的方式来获取 pwd 字符串的长度，从而降低攻击难度。并且密码明文存储，也可能泄露。

①: 使用 challenge-response scheme 来验证登录密码，即不发送 pwd 本身。

②: 在获取输入密码内容时不通过 while-break 的方式而是通过先获取长度再循环的方式。

③: 添加 salt 即以 hash 密文形式与 database 中数据比较。

④: 在可信的安全系统中进行 login 认证，通过 guard 防止 attacker 的计时攻击。

上海交通大学答题纸

（2022至2023学年第1学期）

5200210227 9

课程名称 CSE 姓名 李昊翰

3、1. 若 i%3==0：

variable	taint status
i	true
a	false
j	true
k	true

若 i%3!=0：

variable	taint status
i	true
a	false
j	false
k	false

4. remove_taint(uint16 v)

```
{
    uint16 ans=0
    while(v!=0){
        ans++;
        v--; // v 每有1个1, ans 就+1, 最终 ans=v.
    }
    return ans;
}
```

5. ①: shadow stack: 是一个只用于存储 return address 的 stack, 其会在一个新的 return 时当真正的 stack 同时 push 相同的 return address 入栈, 并在 return 时同时 pop, 只有两者 pop 内容相同才会跳转, 否则会报错

②: CFI: 即 control flow integrity, 即通过预先确定一个 application 的 control-flow graph 来确定一个程序执行流, 若出现不一致会报错, 是一种 static analysis.

③: shadow stack drawback: 需要额外的 push, pop, 性能较差

④: CFI: drawback: 无法防御未修改控制流的攻击。

上海交通大学答题纸

（20 22 至 20 23 学年 第 1 学期）

课程名称 CSE

姓名 李昱翰 5200219102?9

6、Q: 可以使用同态加密。

A: 同态加密适用于用户只有数据而无运算资源，而 untrusted cloud 有充足运算资源的场景。同态指的是 w data 运算后加密与加密后运算结果相同。虽然目前运算并不是所有运算都用同态加密，但是此此问题中的加法，乘法可以满足，故可以使用此方法进行加密。