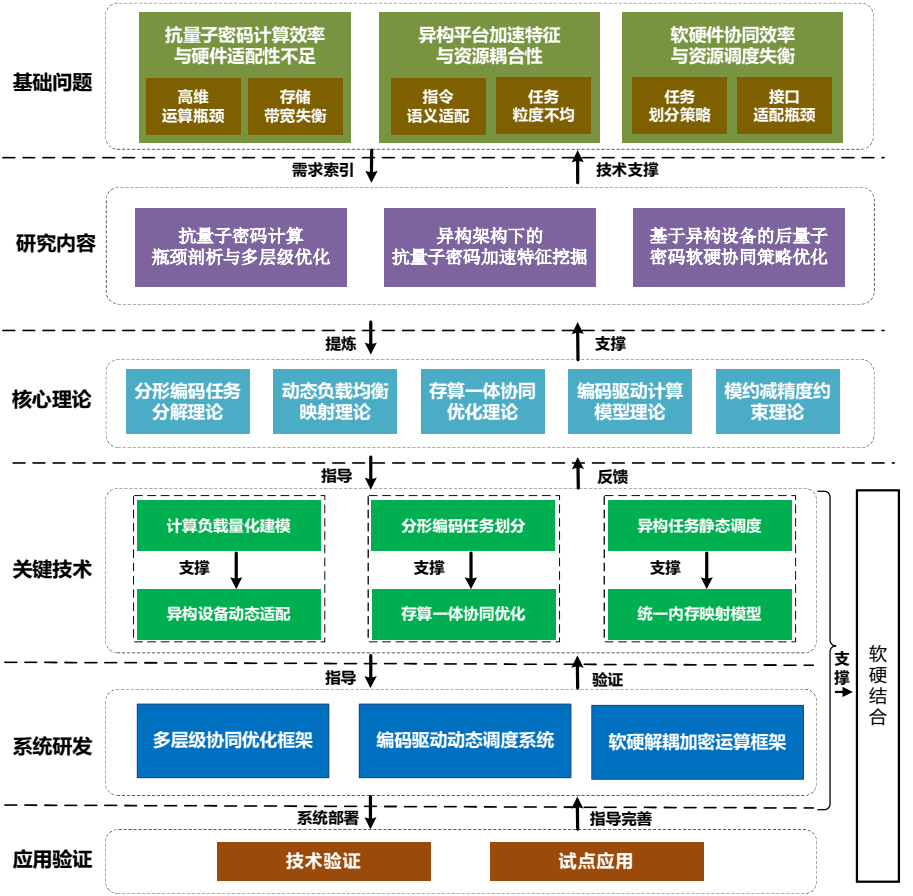

基础问题
抗量子密码计算效率与硬件适配性不足
高维运算瓶颈
存储带宽失衡
异构平台加速特征与资源耦合性
指令语义适配
任务粒度不均
软硬件协同效率与资源调度失衡
任务划分策略
接口适配瓶颈
需求索引
技术支撑
研究内容
抗量子密码计算瓶颈剖析与多层级优化
异构架构下的抗量子密码加速特征挖掘
基于异构设备的后量子密码软硬协同策略优化
提炼
支撑
核心理论
分形编码任务分解理论
动态负载均衡映射理论
存算一体协同优化理论
编码驱动计算模型理论
模约减精度约束理论
指导
反馈
关键技术
计算负载量化建模
支撑
异构设备动态适配
分形编码任务划分
支撑
存算一体协同优化
异构任务静态调度
支撑
统一内存映射模型
支撑
软硬结合
指导
验证
系统研发
多层级协同优化框架
编码驱动动态调度系统
软硬解耦加密运算框架
系统部署
指导完善
应用验证
技术验证
试点应用

图 1 软硬结合研究内容

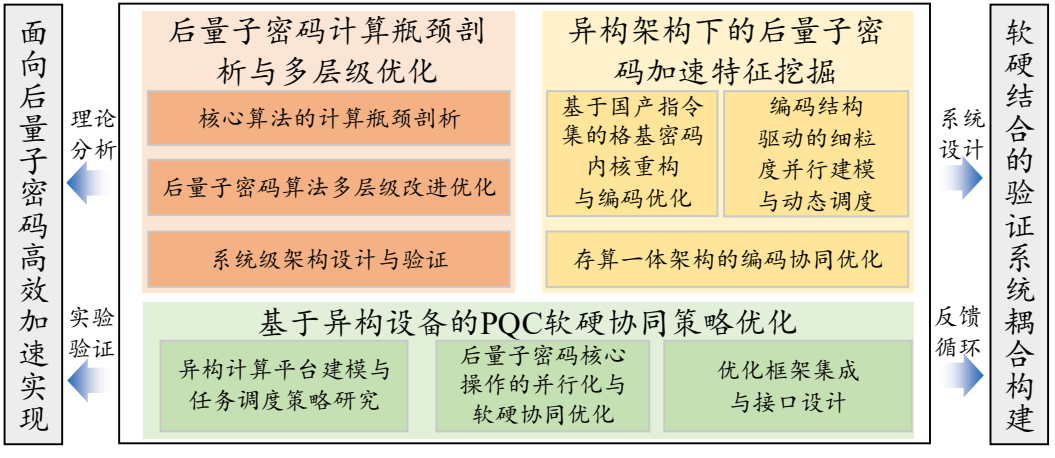


图 1 后量子密码加速实现框架

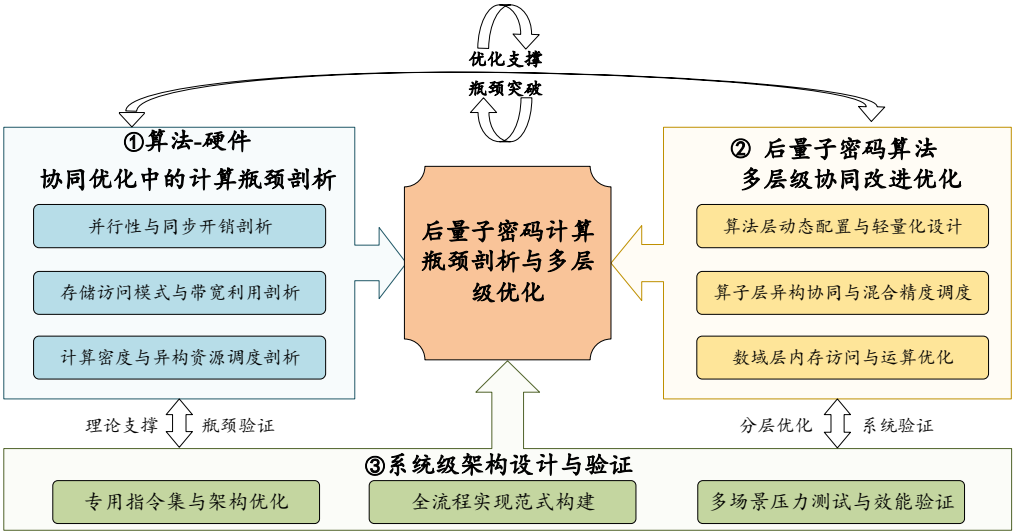


图 2 后量子密码计算瓶颈剖析与多层级优化

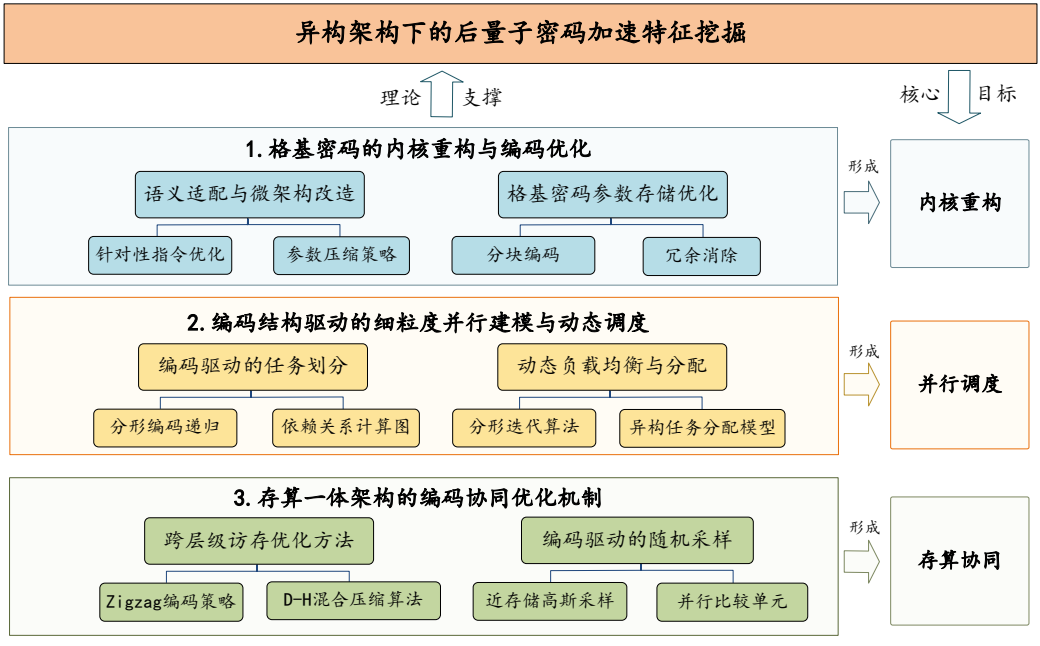


图 3 异构架构下的后量子密码加速特征挖掘

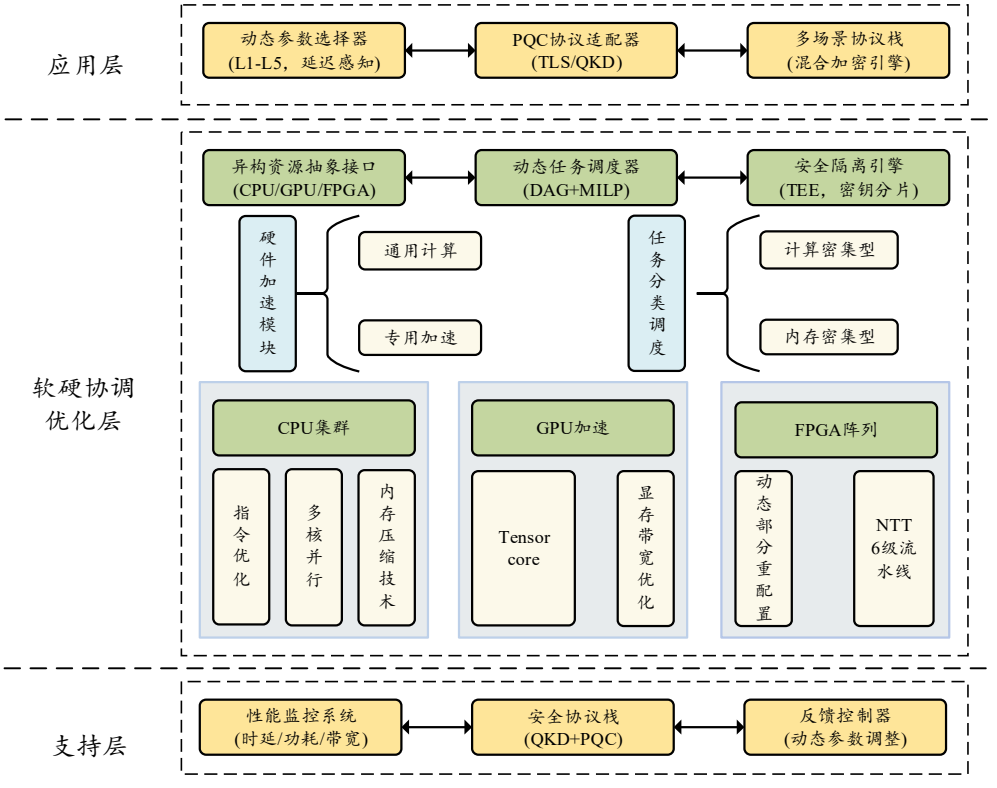


图 4 异构芯片架构下后量子密码软硬协同策略优化

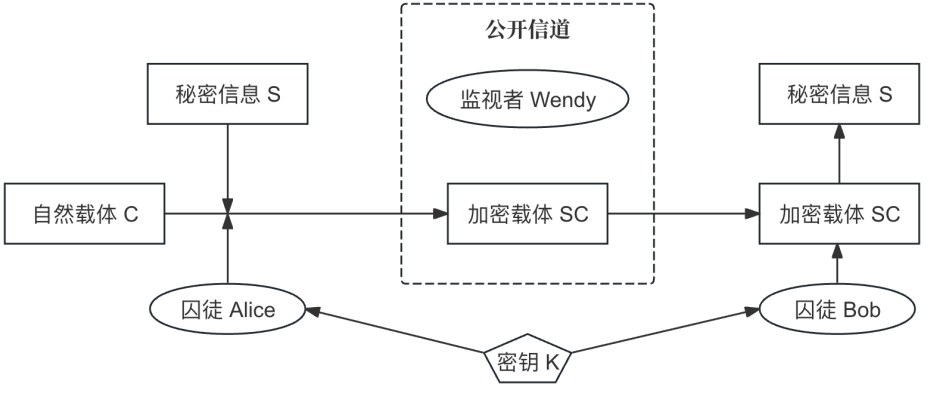

公开信道
秘密信息 S
监视者 Wendy
秘密信息 S
自然载体 C
加密载体 SC
加密载体 SC
囚徒 Alice
囚徒 Bob
密钥 K

图 1.1 “囚徒模型”示意图

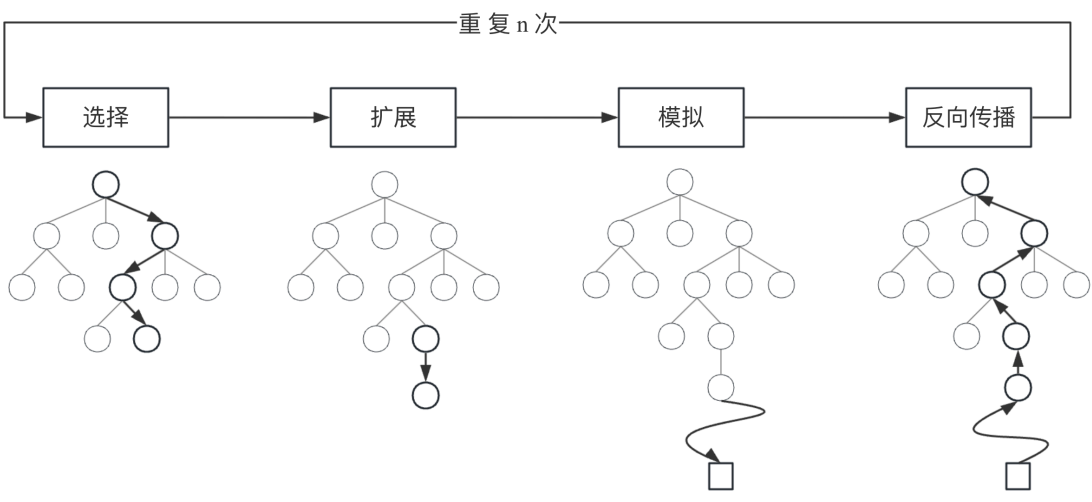


图 3.2 蒙特卡洛树扩充流程

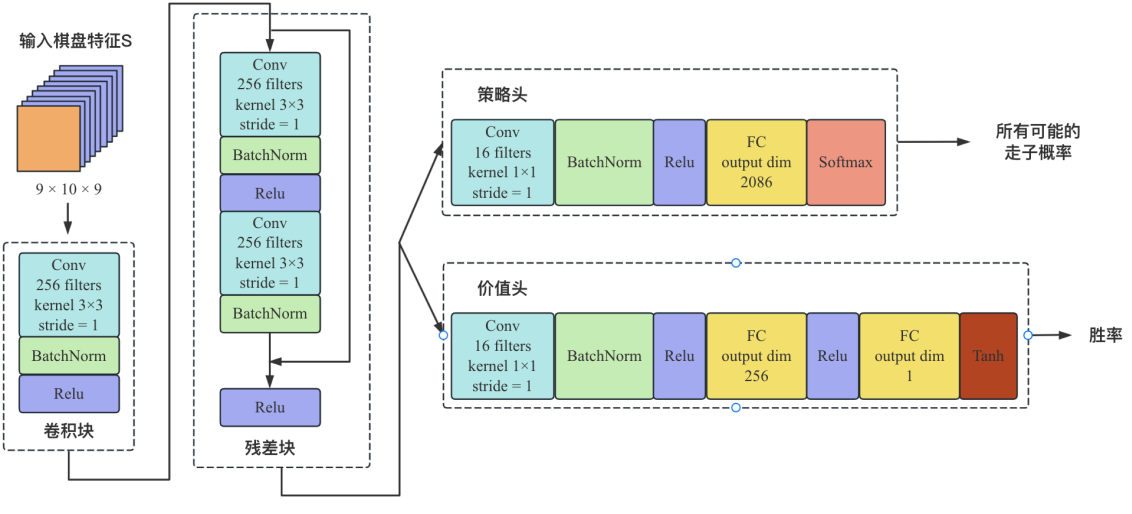

输入棋盘特征S
9 × 10 × 9
Conv
256 filters
kernel 3×3
stride = 1
BatchNorm
Relu
卷积块
Conv
256 filters
kernel 3×3
stride = 1
BatchNorm
Relu
Conv
256 filters
kernel 3×3
stride = 1
BatchNorm
Relu
残差块
策略头
Conv
16 filters
kernel 1×1
stride = 1
BatchNorm
Relu
FC
output dim
2086
Softmax
所有可能的
走子概率
价值头
Conv
16 filters
kernel 1×1
stride = 1
BatchNorm
Relu
FC
output dim
256
Relu
FC
output dim
1
Tanh
胜率

图 3.3 策略价值网络

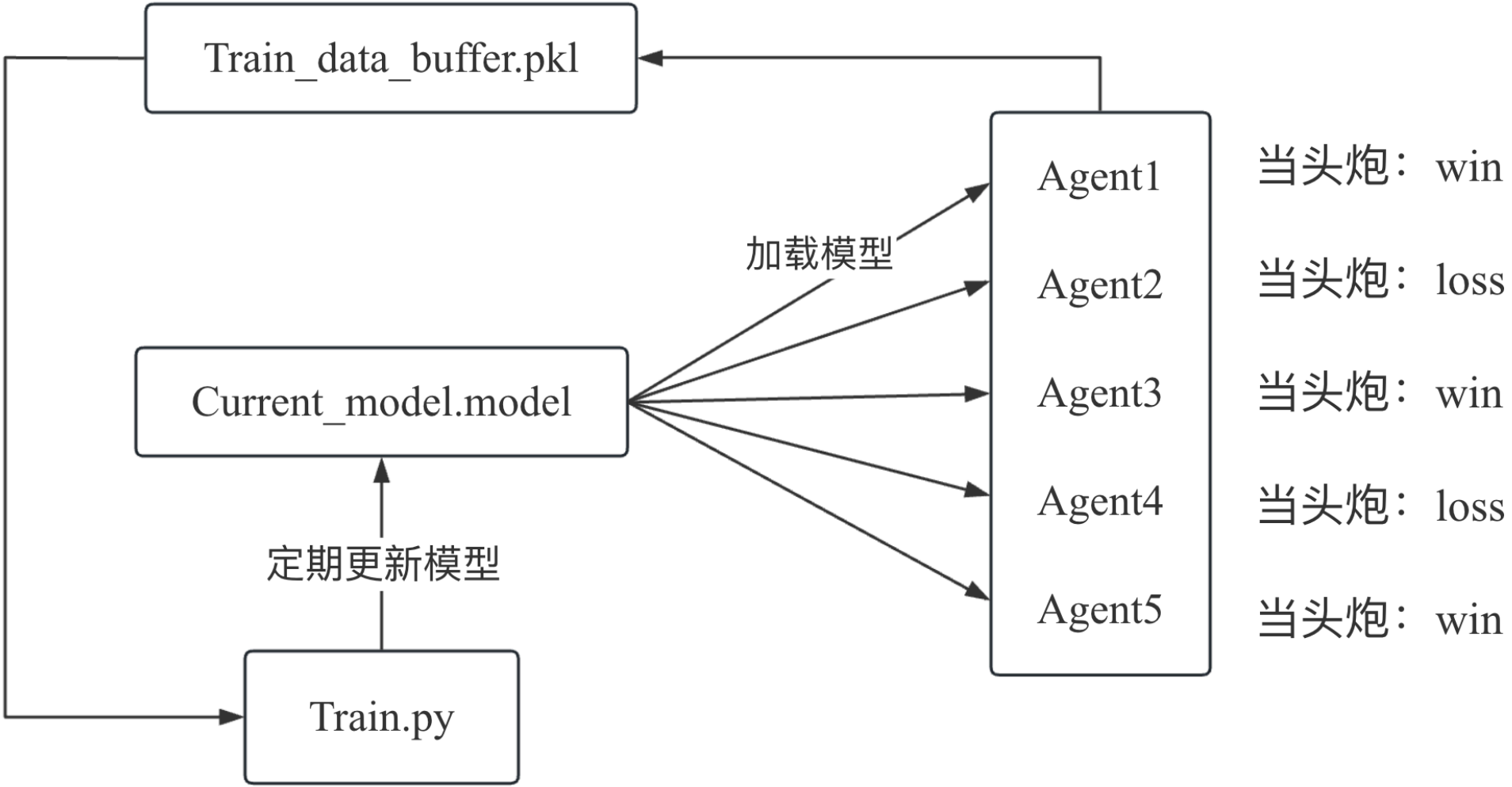
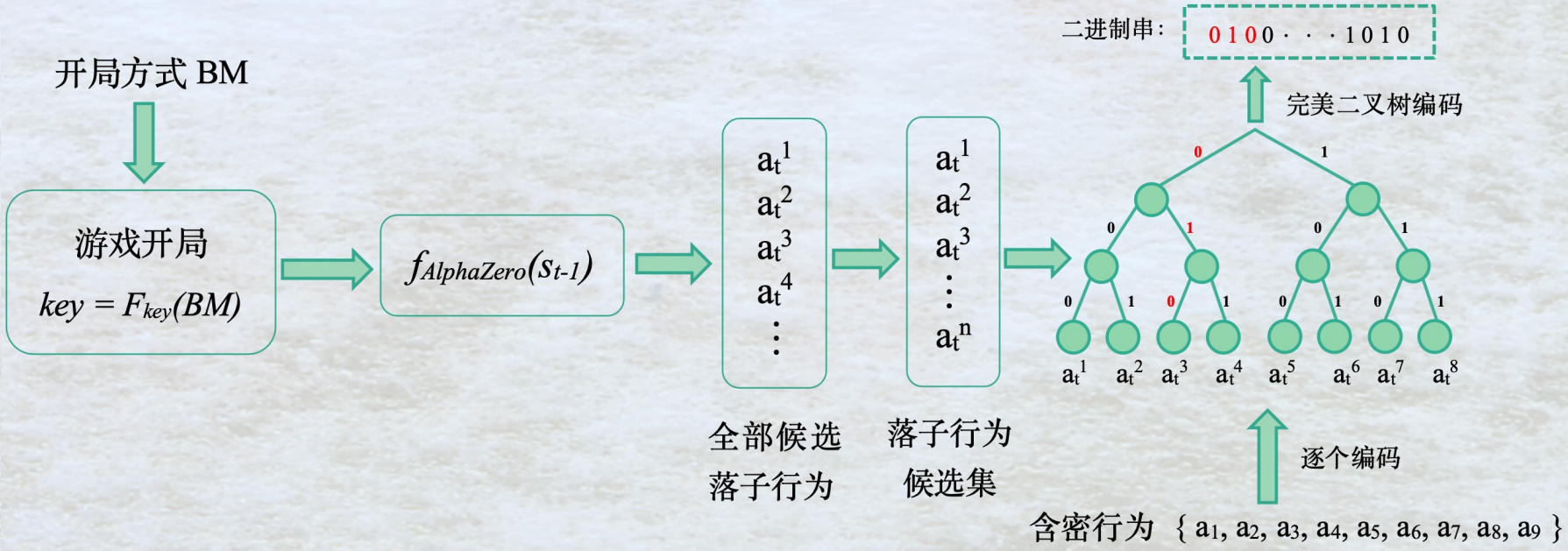

Train_data_buffer.pkl
Agent1
当头炮：win
加载模型
Agent2
当头炮：loss
Current_model.model
Agent3
当头炮：win
Agent4
当头炮：loss
定期更新模型
Agent5
当头炮：win
Train.py

图 3.4 并行训练示意图

2.3 算法具体流程



其中s_{t-1}表示当前棋盘状态，a_t^i 表示第t次落子行为，在SPM中排在第i个