Suggested Projects

Scientific Computing: CN 406

Note: You may propose a topic of your own if none of the topics below interests you . In such a case, you must consult with me about the topic you wish to present.

1 Computational Science

1. Various number factoring algorithms: Pollard's $p-1$ algorithm, Elliptic curve method, Quadratic sieve, Number field sieve, Continued fraction method, Lattices...
2. Various prime counting algorithms: Sieve of Eratosthenes, Legendre's formula ...
3. Application of neural network in scientific computing
4. Symbolic computing and computing algebra systems
5. Various global optimization techniques: Evolutionary algorithms, Genetic algorithms, Ant Colony, Particle swarm, Hill Climbing, Simulated annealing, Dynamic Programming ...
6. Various graph/tree search algorithms: A star, Dijkstra's algorithm, Tree pruning ...
7. Parallel and distributed computing

2 Theoretical Computer Science

1. Random numbers and pseudorandom number generators
2. Zero knowledge proof
3. Quantum computing
4. Computational complexity theory ($NP = P?$)
5. Fuzzy logic

3 Cryptography

1. Hash functions
2. Secret sharing scheme/identification scheme
3. Elliptic curve cryptography
4. Hyperelliptic curve cryptography
5. Various digital signature schemes: RSA, GGH, ElGamal, NTRU ...
6. Various public cryptosystems: NRTU, knapsack ...
7. Modern symmetric cryptosystems: DES and AES