CMSC 711 Computer Networks **Spring 2018**

Final Exam

Open book and notes; Take home *Due: Wednesday, May 16th, noon.*

- I cannot stress this point enough: **Be precise**. If you have written something incorrect along with the correct answer, you should **not** expect to get all the points. I will grade based upon what you **wrote**, not what you **meant**.
- Please do not quote papers verbatim. Explain requested concepts with your own words and examples.
- Maximum possible points: 100 + bonus.

Problem	Grade
General	
Deployed Systems	
Wireless/Coding	
Privacy/Auctions	
Design	
Total	

- General
  - How is the `newLeafs(leafSet)` call used in Pastry? When is it invoked? (Don't simply quote the paper) (4 points)
  - Extend the Zmap permutation procedure such that it can be run on k machines in parallel. Explain the properties of your protocol. (6 points)
- Deployed Systems
  - Describe how *adding* a new provider can reduce global anycast performance. (3 points)
  - How does the γ parameter in the "Majority is not Enough..." relate to the underlying network topology? (3 points)
  - What steps of the Tor circuit creation protocol uses its PKI (directory service)? Why? What is the underlying security assumption about the PKI? (4 points)
- Wireless/Coding
  - Are Spinal codes rateless? Describe why or why not? (3 points)
  - (Why) do LT codes require nodes of low degree in the encoding graph? What is the minimum required degree and why? (3 points)
  - In the "Cooperative Security for Network Coding..." paper, (how) can an adversary generate hash collisions if it knew values of the form $g_i^{x_i} = g_j^{x_j}$? (4 points)
- Privacy/auctions
  - (How) Can a bidder and the ad-exchange collude to influence auctions in VEX? (3 points)
  - What is a potential problem sampling n random "rows" in Split-X? (3 points)
  - Describe a change to Split-X that would make it not be susceptible to this problem. (4 points)
- Design

  Cellular devices have an unique identifier that network providers can map to real-world identities. Providers can track users' locations by recording cell tower association(s).

  Design a protocol that will preserve user privacy, i.e., providers should not learn whom a user calls, how long their calls are, and where users are at any time. The current user-user and user-provider interface should be preserved to the extent possible (i.e., users should be able to add others as contacts, roam, and call others at any time, and providers should be able to charge by talk-time if they wish).

  Along with your protocol specification, list all hardware and software changes you will require. List the properties you wish to provide and discuss to what extent your protocol provides these properties. Discuss the limitation of your protocol. (10 points)

Number of calories in a Peach Lemonade (8 oz.): 6 60 160 (1 point)